**DATA PROCESSING ADDENDUM**

1. This Data Processing Addendum ("**Addendum**") forms part of the the User Agreement for "Guesty for Host" ("**Principal Agreement**") between: (i) Guesty, Inc. located at 340 S Lemon Ave. #9720 Walnut, CA 91789 a Delaware corporation **(**"**Vendor**"**)** acting on its own behalf and as agent for each Vendor affiliate; and (ii) the customer listed on the Principal Agreement ("**Company**").

2. In consideration of the mutual obligations set out herein, the Parties hereby agree that the termsand conditions set out below shall be added as an Addendum to the Principal Agreement. Exceptwhere the context requires otherwise, references in this Addendum to the Principal Agreementare to the Principal Agreement as amended by, and including, this Addendum. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

3. Under the Principal Agreement the nature and purposes of processing Personal Data by the Vendor as data processor shall be limited to those set forth in **Schedule 1**.

4. **Definitions**

4.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

4.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company 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 is subject to any other Data Protection Laws;

4.1.2 "**Company Personal Data**" means any Personal Data Processed by Vendor on behalf of a Company pursuant to or in connection with the Principal Agreement;

4.1.3 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

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

4.1.5 "**EU Data Protection Laws**" means the UK General Data Protection Act 2018, EU General Data Protection Regulation 2016/679, as transposed into domestic legislation of each Member State, each as amended, replaced or supersededfrom time to time;

4.1.6 "**Restricted Transfer**" means:

4.1.6.1 a transfer of Company Personal Data from any Company to Vendor; or

4.1.6.2 an onward transfer of Company Personal Data from Vendor to a Sub-processor, or between two establishments of Vendor,

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 the Standard Contractual Clauses to be established under Section 16.1 below;

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

4.1.8 "**Standard Contractual Clauses**" means the contractual clauses set out in Schedule 2, amended as indicated (in square brackets and italics) in that Schedule;

4.1.9 "**Sub-processor**" means any person (including any third party and any Vendor affiliate, 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 the Company in connection with the Principal Agreement; and

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

4.1.11 "**Party**"/"**Parties**" means the Company and the Vendor separately, or jointly, as the case may be;

4.1.12 "**Purpose**" means as described in Schedule 1; and

4.1.13 "**Supervisory Authority**" means any court, regulatory agency or authority which, according to Applicable Laws and/or regulations, supervises privacy issues and/or the processing of personal data.

4.2 The terms, "**commission**", "**controller**", "**data subject**", "**member state**", "**personal data**", "**personal data breach**", "**processing**", "**processor**" and "**supervisory authority**" shall have the same meaning as in the EU Data Protection Laws, and their cognate terms shall be construed accordingly.

5. **Special undertakings of the Parties**

5.1 **Roles, ownership of personal data, processing and purpose**

5.1.1 The Company shall be considered the controller of the personal data processed on its behalf and in accordance with its instructions, which concerns its respective data subjects. The Vendor shall be considered a processor of the personal data processedon behalf of the Company.

5.1.2 The Vendor may only process the Company Personal Data for the Purpose and to the extent it is necessary for the fulfilment of the Vendor's obligations under this Addendum or the Principal Agreement.

5.1.3 This Addendum shall apply to the actions of any of Vendor or Company's affiliates performing tasks and obligations in the context of this Addendum and any such affiliates shall have all rights and obligations set forth in this Addendum as if they were Vendor or Company, as applicable.

5.2 Special undertakings of the Company

5.2.1 The Company undertakes to:

(a) Ensure that there is a legal ground for processing the personal data covered bythis Addendum;

(b) Ensure that any disclosure or transfer of Company Personal Data to Vendor confirms to the Applicable Laws.

(c) Inform the Vendor about any erroneous, rectified, updated or deleted personaldata subject to the Vendor's processing; and

(d) Fully comply with any request of data subjects and with any data subject rights under Applicable Laws.

(e) Provide the Vendor with documented instructions regarding the Vendor's processing of the personal data, as may be required from time to time.

5.3 Special undertakings of the Vendor

5.3.1 **The Vendor undertakes to:**

(a) Only process the Company Personal Data in accordance with Applicable Laws and the Company documented instructions, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Applicable Laws; in such a case, the Vendor shall inform the Company of that legal requirement before processing the personaldata, unless such information is prohibited by the Applicable Laws on important grounds of public interest;

(b) Taking into account the nature of the processing, implement appropriate technical and organisational measures to reasonably ensure a level of security appropriate to the risk and reasonably assist the Company by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights or with respect to data breaches in Applicable Laws; and

(c) Make available to the Company all information reasonably necessary to demonstrate compliance with the obligations laid down in this Addendum.

6. **Processing of Company Personal Data**

6.1 The Company instructs Vendor (and authorises Vendor to instruct each Sub-processor) to process Company Personal Data and transfer Company Personal Data to any country or territory as reasonably necessary for the provision of the Services and consistent with the Principal Agreement.

6.2 Schedule 1 to this Addendum sets out certain information regarding the Vendor's processing of the Company Personal Data. Company shall immediately inform Vendor of any required amendments to Schedule 1 by written notice to Vendor, and the Parties shall negotiate in good-faith the amendment of Schedule 1.

7. **Confidentiality**

7.1 Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Vendor who may have access to the Company Personal Data, and to ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

8. **Data Security**

8.1 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 reasonably ensure a level of security appropriate to that risk.

9. **Sub-processing**

9.1 Company authorises Vendor to appoint (and permit each Sub-processor appointed in accordance with this Section 9 to appoint) Sub-processors in accordance with this Section 9 and any restrictions in the Principal Agreement.

9.2 Vendor may continue to use those Sub-processors already engaged by Vendor as at the date of this Addendum, as listed on the Vendor's website, subject to Vendor meeting the obligations set out in Section 9.4.

9.3 Vendor shall give Company prior written notice of the appointment of any new Sub-processor. If, within 7 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

9.3.1 Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and

9.3.2 where such a change cannot be made within 30 days from Vendor's receipt of Company's notice, the Company shall be responsible to find an alternative Sub-processor that accepts to provide services to Vendor under similar conditions than the Sub-processors objected by Company. In the event such proposed alternative Sub-processor is not accepted by Vendor, then Company may by written notice to Vendor with immediate effect terminate the Principal Agreement to the extent thatit relates to the Services which require the use of the proposed Sub-processor.

9.4 With respect to each Sub-processor, Vendor shall:

9.4.1 ensure that the arrangement between the Vendor, and the Sub-processor, 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 Addendum; and

9.4.2 if that arrangement involves a Restricted Transfer, ensure that adequate safeguards are put in place to address such Restricted Transfer in accordance with applicable rules for international data transfers, for example through use of the Standard Contractual Clauses Vendor and the Sub-processor.

9.5 Vendor shall ensure that each Sub-processor performs the obligations under this Addendum, as they apply to processing of Company Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of Vendor.

10. **Data subject rights**

10.1 Vendor shall:

10.1.1 promptly notify Company if Vendor receives a request from a data subject under any Data Protection Law in respect of Company Personal Data; and

10.1.2 ensure that the Vendor does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Vendor is subject.

11. **Personal Data Breach**

11.1 Vendor shall notify Company without any delay but no later than within 48 hours in writing upon Vendor or any Sub-processor becoming aware or has reasons to believe of a Personal Data Breach affecting Company Personal Data, providing Company with reasonably sufficient information to allow Company to meet its obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

11.2 Immediately following Vendor's notification to Company of a Personal Data Breach, the Parties shall coordinate with each other to investigate the breach. Vendor agrees to reasonably cooperate with Company, at Company's expense, in Company's handling of the matter, including, without limitation:

11.2.1 assisting with any investigation;

11.2.2 facilitating interviews with Vendor's employees and others involved in the matter; and

11.2.3 making available all reasonably necessary records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Company.

11.3 Vendor agrees to assist Company in advising the Supervisory Authority and data subjects about Personal Data Breach. It shall not, however, inform any third party of any Personal Data Breach without first obtaining Company's prior written consent, other than to inform a complainant (if any) that the matter has been forwarded to Company, or if otherwise required under any Applicable Law.

11.4 Company shall reimburse Vendor for actual reasonable costs incurred by Vendor in responding to, and mitigating damages caused by any security incident or Personal Data Breach, including all costs of notice and/or remediation.

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

12.1 Vendor shall provide reasonable assistance to Company, at Company's expense, with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, 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 Vendor.

13. **Cooperation and Coordination**

13.1 Upon reasonable request by Company, Vendor shall as promptly and as reasonably practicable provide Company with a written report containing information reasonably requested by Company relating to: (i) any security event and Personal Data Breach; or (ii) actual or reasonably suspected non-compliance with this Addendum. In addition, Vendor shall provide Company with any documents reasonably requested by Company related to the foregoing,

including without limitation, any information security assessment and security control audit reports.

14. **Deletion or return of Company Personal Data**

14.1 Subject to Section 14.2 Vendor shall promptly and in any event within fourteen (14) days of the date of termination or expiration of any Services involving the Processing of Company Personal Data (the "**End Date**"), or of the date of a written notice by Company, delete and procure the deletion of all copies of those Company Personal Data.

14.2 Vendor 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.

15. **Audit rights**

15.1 At the request of Company and on its expense, but not more than once per year, Vendor shall conduct site audits of the information technology and information security controls for all facilities used in complying with its obligations under this Addendum. Company shall treat such audit reports as Vendor's confidential information.

15.2 Company shall have the right to perform audits, not more than once per calendar year and upon prior written notice of at least thirty (30) days to Vendor, of the Vendor's processing of the Company Personal Data in order to verify the Vendor's, and any Sub-processor's, compliance with this Addendum. The audit shall be confined to processing documentation prepared by the Vendor and logged and documented information regarding its information security measures, and in any event will not entitle Company to conduct technological investigations on the Vendor's information systems.

15.3 Company shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Vendor's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

15.4 If any Supervisory Authority: (i) contacts the Vendor with respect to its systems or any processing of Company Personal Data carried out by the Vendor, (ii) conducts, or gives notice of its intent to conduct, an inspection of the Vendor with respect to the processing of Company Personal Data, or (iii) takes, or gives notice of its intent to take, any other regulatory action alleging improper or inadequate practices with respect to any processing of Company Personal Data carried out by the Vendor, then the Vendor shall immediately notify the Company and shall subsequently supply the Company with all information pertinent thereto to the extent permissible by law.

15.5 Company shall bear all costs for audits set out in this Addendum.

16. **Restricted Transfers**

16.1 In the event that the processing activities under this Addendum are considered Restricted Transfer, the Company (as "data exporter") and Vendor, (as "data importer") hereby enter into the Standard Contractual Clauses included in **Schedule 2** in respect of any Restricted Transfer from that Company to Vendor.

16.2 Before the commencement of any Restricted Transfer to a Sub-processor, Vendor will have put in place appropriate measures for any such transfer of Personal Data to ensure that the level of protection of natural persons guaranteed by EU Data Protection Laws is not undermined, including the use of Standard Contractual Clauses.

17. **General Terms**

17.1 *Governing law and jurisdiction*

Without prejudice to Mediation and Jurisdiction and Governing Law sections of the Standard Contractual Clauses:

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

17.1.2 this Addendum 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 forthis purpose in the Principal Agreement.

17.2 *Assignation of rights or obligations*

Neither Party may assign its rights or obligations under this Addendum without the prior written consent of the other Party.

17.3 *Notices*

All notices to a Party under this Addendum shall be in writing and sent to its address as set forth at the beginning of this Addendum, or to such other address as such Party has provided the otherin writing for such purpose. Notices may be sent by post, courier, fax or email.

Notices shall be deemed to have been duly given (i) on the day of delivery when delivered in person or by courier, (ii) three (3) business days after the day when the notice was sent when sent by post, and (iii) on the day when the receiver has manually confirmed that it is received when sent per fax or email.

17.4 *Term and termination*

This Addendum shall enter into force on the date hereof. Unless terminated earlier (i) due to a material breach of the terms of this Addendum, in which case this Addendum shall be terminatedwith immediate effect if the other Party fails to cure such breach in a satisfactory manner withinfifteen (15) days after the other Party's written demand thereof, or (ii) this Addendum shall remain in force until the termination or expiration of the Principal Agreement, whereupon it shall terminate automatically without further notice. The termination or expiration of this Addendum shall immediately terminate any processing agreement entered into between Vendorand any Sub-processor.

Either Party may terminate this Addendum by giving the other Party thirty (30) days written notice.

17.5 *Liability and indemnification*

Each Party shall indemnify and hold the other Party harmless from and against all losses due

to claims from third parties including government/authority fines and penalties resulting from arising out of or relating to any breach by such first-mentioned Party of the this Addendum and in the applicable Data Protection Laws.

Any loss suffered by a Party resulting from, arising out of or relating to a breach of this Addendum by the other Party that is not due to claims from third parties under Section 16.7 shall be governed by the provisions regarding liability and limitation of liability in the Principal Agreement.

## SCHEDULE 1

## DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

### 1. THE PROJECT

Guesty For Host is a software management platform provided by Vendor for short-term and vacation rentals. Processing of Company Personal Data is for the purpose of assisting property management companies, property owners and guests and simplifying their managing their vacation.

### 2. DATA SUBJECTS

The Company Personal Data processed concern the following categories of data subjects:

Customers, employees, consumer customers and/or representatives of corporate customers andsuppliers.

### 3. CATEGORIES OF PERSONAL DATA

The Company Personal Data processed concern the following categories of personal data:

Name, gender, phone number, address, email address, company name and VAT number, personalidentification number, credit card information, device information, IP number, location tracking.

We may also collect feedback, comments and questions received in service-related communication and activities, such as meetings, phone calls, documents, and emails.

### 4. PURPOSE OF THE PERSONAL DATA PROCESSING

We collect and use the Company Personal Data to provide the services as described in the Principal Agreement, which includes the provision of the software management platform to Customer, providing customer support, as well as other operational activities with respect to the managed properties, on behalf of the Company and upon Company’s instructions.

## SCHEDULE 2

## STANDARD CONTRACTUAL CLAUSES (MODULE 2 - CONTROLLER TO PROCESSOR)

### SECTION I

***Clause 1***

**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) Company (hereinafter 'data exporter'), and

(ii) Vendor (hereinafter 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***Clause 2***

**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3***

**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e); and

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4***

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6***

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7***

**Docking clause**

*[Intentionally left blank]*

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the

data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

***Clause 9***

**Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to

instruct the sub-processor to erase or return the personal data.

***Clause 10***

**Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

***Clause 11***

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12***

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

***Clause 14***

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Clause 15***

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

***Clause 16***

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***Clause 17***

**Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Netherlands.

***Clause 18***

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**ANNEX I**

*[intentionally left blank]*

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*
As described in the Addendum

*Categories of personal data transferred*
As described in the Addendum

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*
N/A

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*
Continuous.

*Nature of the processing*
Provision of services.

*Purpose(s) of the data transfer and further processing*
As described in the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*
For as long as necessary for the performance of the services, as further described in the Agreement and Addendum.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*
For hosting and support functions, on a continous basis.

**C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority is Autoriteit Persoonsgegevens, The Netherlands .

**ANNEX II**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

As described in the Addendum.