DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between Customer **("Customer" or "Controller")** and HqO Inc., and its affiliates and subsidiaries worldwide **("Vendor" or "Service Provider"**) and forms part of the Master Terms and Conditions entered into by and between Customer and Vendor through the related Order Form thereto (the "**Agreement**"). Customer and Vendor are each a "**Party**" and together the "**Parties**."

BACKGROUND

WHEREAS, Vendor provides certain services to Customer in accordance with the Agreement ("**HqO Service**"); and

WHEREAS, this DPA governs the Processing of certain Customer Data and Personal Data by Vendor in connection with its provision of the Services.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

Definitions. Unless otherwise defined in the Agreement, the following definitions apply in this DPA:

1. **"Customer Data" has the meaning ascribed to that term in the Agreement.**
2. **"Personal Data" means any information relating to an identified or identifiable natural person**

Processed by Vendor in the course of providing the Services to Customer. Without limiting the foregoing, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Vendor shall not acquire any right, title or interest in or to Personal Data of Customer.

3. "Processing" (and its variants) means any operation or set of operations performed on Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

4. "Data Privacy Laws" means (as applicable to the Personal Data Processed by the Vendor) all laws in relation to (a) data protection; (b) privacy; (c) interception and monitoring of communications; (d) restrictions on, or requirements in respect of, the Processing of Personal Data of any kind; and (e) actions required to be taken in respect of unauthorized or accidental access to or use or disclosure of Personal Data, and includes without limitation: the Personal Information Protection and Electronic Documents Act, SC 2000, c 5, the Alberta Personal Information Protection Act, SA 2003, c P-6.5, the British Columbia Personal Information Act, SBC 2003, c 63, and the Quebec Act respecting the protection of personal information in the private sector, CQLR c P-39.1; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), the UK Data Protection Act of 2018 ("UK GDPR"); and the "California Consumer Privacy Act of 2018," Assembly Bill 375 of the California House of Representatives, an

act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018, including any amendments thereto from time to time, and together with any orders, guidelines and/or instructions issued under any of the above by relevant supervisory authorities or courts of competent jurisdiction.

5. "New EU SCCs" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, completed as set forth in Schedule A to this DPA.

6. "Old EU SCCs" means the Standard Contractual Clauses issued pursuant to EU Commission Decision of 5 February 2010 *on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council* (available as of the Effective Date at http://data.europa.eu/eli/dec/2010/87/2016-12-17).

7. "Subprocessor" means any third-party engaged by Vendor to Process Personal Data on Vendor's behalf in connection with providing the services under the Agreement.

Data Protection Obligations

1. **Compliance with Laws.** Vendor shall comply with all applicable Data Privacy Laws, rules and regulations in relation to the Processing of Personal Data under the Agreement and this DPA. If Vendor determines that it can no longer meet its obligations under this DPA or applicable Data Privacy Laws, Vendor shall immediately notify Customer, stop Processing all Personal Data, and take any other commercially-reasonable remediation measure requested by Customer in good faith.

2. **Instructions.** The Agreement and this DPA sets out the Customer's Processing instructions to Vendor.

Vendor shall only Process Personal Data and Customer Data (i) on behalf of Customer and as necessary for Vendor to provide the Services, (ii) in compliance with Customer's instructions under the Agreement and this DPA and (iii) to comply with applicable law. The Parties agree that Customer may communicate any change in its instructions to Vendor by way of written notification to the Vendor and that Vendor shall abide by such instructions, unless prohibited by applicable Data Privacy Laws. Vendor shall immediately inform the Customer in writing if, in Vendor's opinion, any of Customer's instructions infringes applicable laws or impedes the provision of Services and shall provide a detailed explanation of the reasons for its opinion in writing, unless prohibited by applicable Data Privacy laws from providing such detailed explanation.

3. **Restrictions on Use of Data.**

3.1 The Vendor agrees that the Customer discloses Personal Data to Vendor solely (i) for a valid

business purpose; and (ii) to allow the Vendor to perform the Services.

3.2 Vendor will not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for any purpose

other than providing the Services; and (iii) retain, use, or disclose the Personal Data except as permitted in the Agreement between Vendor and Customer and any agreements between (x) the applicable data subject to which the Personal Data applies.

3.3 Vendor understands the prohibitions outlined in Section 3.

4. **Vendor Personnel.** Vendor will restrict its personnel from Processing Personal Data and/or Customer

Data without authorization. Vendor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. Vendor shall ensure that any personnel who have access to Personal Data have undergone appropriate training to ensure that they understand their data protection responsibilities with respect to Personal Data that they Process on behalf of Customer. Vendor also warrants that any person acting under its authority and with access to Personal Data for the provision of the Services shall Process Personal Data only pursuant to the Agreement and this DPA.

5. **Disclosure requests.**

Vendor will immediately refer to Customer any request received from any relevant supervisory authority under applicable Data Privacy Laws that relate to the Vendor's Processing of Personal Data. Vendor shall cooperate with Customer in its dealings with any supervisory authority concerned and with any audit request received from a supervisory authority concerned. Customer shall be entitled to disclose this DPA or any other document (including contracts with subcontractors) that relate to the performance of its obligations under this DPA provided Vendor has agreed and the parties have cooperated on redacting any confidential or sensitive information.

Vendor will not disclose Personal Data to any third party (including any government agency, court, or law enforcement) except with written consent from Customer or as necessary to comply with applicable law. If Vendor must disclose Personal Data to a law enforcement agency or third party, Vendor shall provide Customer with notice of the access request to allow Customer to seek a protective order or other appropriate remedy. If notice is legally prohibited, Vendor shall protect the Personal Data from unnecessary disclosure as if it were Vendor's own confidential information and shall inform Customer promptly as soon as possible if and when such legal prohibition ceases to apply.

If Vendor receives any request or communication from a data subject that relates to the Processing of his or her Personal Data ("**Data Subject Request**"), Vendor shall (i) not directly respond to the Data Subject Request, (ii) notify Customer without delay upon and no later than five (5) business days after becoming aware of the Data Subject Request and (iii) provide full cooperation, information and assistance according to further instructions from Customer.

If Customer receives a Data Subject Request, Vendor shall provide Customer with full cooperation, information and assistance in addressing the Data Subject Request.

6. **Deletion**. In accordance with the Agreement, Vendor shall securely delete all Personal Data and Customer Data whether in hardcopy or electronic form following any expiration or termination of this Agreement unless storage of Personal Data or Customer Data is required by applicable law, in which case Vendor shall protect the Personal Data and Customer Data as required by this DPA until such time as it is deleted or returned to Customer. For the purposes of this DPA, "delete" means to render permanently incapable of reconstruction.

7. **Subprocessing.** Vendor shall not engage any Subprocessors, processing Customer's or any Tenant's Personal Data, without notice to Customer. Customer declares its prior approval of Provider's use of the Subprocessors indicated in Schedule B to Process Personal Data. Vendor shall provide Customer with at least thirty (30) days' prior notice of any intended change to Appendix 1. Customer shall have the right to raise reasonable objections for a period of thirty (30) days after any such notice of an intended change to Appendix 1. Vendor shall enter into a binding written contract with each Subprocessor, which contract shall impose at least the same level of protection for Personal Data as those in this DPA having regard to the nature of the services provided by the Subprocessor. Vendor shall regularly check and document that the Subprocessor is fulfilling its obligations.

8. **Assistance to Customer.** Vendor shall provide timely assistance to Customer for Customer to comply with its obligations under applicable Data Privacy Laws, including requests from relevant supervisory authorities and government entities, or any requirements to perform data protection impact assessments under applicable Data Privacy Laws.

9. **Audit**. Vendor shall make available to Customer all information necessary to demonstrate compliance with this DPA. Vendor shall, upon reasonable notice, allow for and contribute to on-site inspections by Customer, an independent auditor selected by Customer that is bound by reasonable confidentiality obligations or a data protection authority of Vendor's or any of its subcontractors' data Processing facilities and activities to ensure compliance with this DPA. Such audits shall only occur after 20 business days' notice, shall be performed during normal business hours, and shall not unreasonably interfere with normal business activities of Vendor or any applicable subcontractor. Customer shall bear the reasonable expenses of such audits performed at its request.

10. **Cross-Border Data Transfers**.
Vendor will comply with all Data Privacy laws applicable to Vendor in its role as provider of the HqO Service. Customer will comply with all applicable Data Privacy laws relevant to use of the HqO Service, including by obtaining any consents and providing any notices required under applicable Data Privacy laws for Vendor to provide the HqO Service. Customer will ensure that Customer and Customer's authorized users are entitled to transfer the Personal Data to Vendor so that Vendor and its Subprocessors may lawfully Process the Personal Data in accordance with this Addendum.

Customer authorizes Vendor and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as applicable Data Privacy law for such transfers is respected.

With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, and such law permits use of the Old EU SCCs but not use of the New EU SCCs, the Old EU SCCs form part of this DPA and take precedence over the rest of this DPA as set forth in the Old EU SCCs, until such time that the United Kingdom adopts the New EU SCCs, in which case the New EU SCCs as provided

herein will control. For purposes of the Old EU SCCs, they shall be deemed completed as follows:

The “exporters” and “importers” are the Parties and their Affiliates to the extent any of them is involved in such transfer, including those set forth in Annex I.A of the New EU SCCs.

i. Clause 9 of the Old EU SCCs specifies that United Kingdom law will govern the Old SCCs.

ii. The content of Appendix 1 of the Old EU SCCs is set forth in Annex I.B of the New EU SCCs herein.

iii. The content of Appendix 2 of the Old EU SCCs is set forth in the Annex II.

With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the New EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

With respect to Personal Data transferred from the European Economic Area, the New EU SCCs incorporated herein as Schedule A shall apply, form part of this Addendum, and take precedence over the rest of this Addendum as set forth in the New EU SCCs.

11. **Additional Safeguards for the Transfer and Processing of Personal Data from the EEA, Switzerland, and the United Kingdom**. To the extent that Vendor Processes Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the European Economic Area, Switzerland, or the United Kingdom, Vendor agrees to the following safeguards to protect such data to an equivalent level as applicable Data Protection Laws:

Customer and Vendor shall encrypt all transfers of the Personal Data between them, and Vendor shall encrypt any onward transfers it makes of such personal data, to prevent the acquisition of such data by third parties, such as governmental authorities.

Vendor represents and warrants that:

i. As of the date of this contract, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a (“FISA Section 702”).

ii. No court has found Vendor to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

iii. It is not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to FISA Section 702.

Vendor will not comply with any request under FISA Section 702 for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).

Vendor will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

Vendor will take no action pursuant to U.S. Executive Order 12333.

At 12-month intervals or more often if allowed by law, Vendor shall, upon Customer's request, provide a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.

Vendor will promptly notify Customer if Vendor can no longer comply with the clauses in this Section. Vendor shall not be required to provide Customer with specific information about why it can no longer comply, if providing such information is prohibited by applicable law. Such notice shall entitle Customer to terminate the Agreement (or, at Customer's option, affected statements of work, order forms, and like documents thereunder) and receive a prompt pro-rata refund of any prepaid amounts thereunder. This is without prejudice to Customer's other rights and remedies with respect to a breach of the Agreement.

12. **Security**. Vendor shall implement appropriate physical, technical and organizational measures to protect Personal Data and Customer Data against unauthorized or unlawful Processing. The measures shall ensure a level of security appropriate to the risk, including as appropriate: (i) pseudonymization and encryption of Personal Data and Customer Data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (iii) the ability to restore the availability and access to Personal Data and Customer Data in a timely manner in the event of a physical or technical incident, and (iv) regular testing, assessing and evaluating the effectiveness of physical, technical and organizational measures for ensuring the security of any Processing for the purpose of providing the HqO Service. Vendor's security measures shall remain at least as robust as those contained at the following link: https://www.hqo.com/security-practices/.

13. **Notification of Personal Data Breach**. Vendor shall notify Customer without undue delay after becoming aware of or reasonably suspecting any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data or Customer Data ("**Data Breach**"). Promptly after discovery or notice of a Data Breach, Vendor shall, at its own costs and expenses, take corrective action to mitigate the Data Breach and to protect the Personal Data and Customer Data from further compromise. Vendor shall provide reasonable information, cooperation and assistance to Customer in relation to a Data Breach of Customer Data and Personal Data, including regarding any communication of the Data Breach to data subjects and Supervisory Authorities.

14. **Miscellaneous.**

1. Notwithstanding anything to the contrary in this DPA or the Agreement, the liability of Vendor for any breach of this DPA shall be subject to the limitations of liability provisions included in the Agreement unless otherwise specified hereunder.

2. The parties acknowledge and agree that the activities performed by Vendor under this DPA do not involve any right to specific compensation other than that compensation owed to Customer for the supply of HqO Service in accordance with the Agreement.

3. Except as mandated under applicable Data Privacy Laws, any dispute relating to this DPA shall be governed by and interpreted in accordance with the law of the country and subject to the jurisdiction referred to in the Agreement.

Schedule A

STANDARD CONTRACTUAL CLAUSES

SECTION 1

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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each '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);

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

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the

case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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.

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 organizational 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 its 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 organizational 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 authorized 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 Union2 (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, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting 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 defense 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 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) GENERAL WRITTEN AUTHORISATION 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 30 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.

[2] 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.

(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[3]. The Parties agree that, by complying with this Clause, the data importer fulfills 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 fulfill 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 authorized 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 organizational 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 authorized 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, organization 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.

[3] This requirement may be satisfied by the sub-processor accessing these Clauses under the appropriate Module, in accordance with Clause 7.

(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) (i) [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.

(ii) [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 behavior 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 authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organizational 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 fulfill its obligations under these Clauses,

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

the data exporter shall promptly identify appropriate measures (e.g. technical or organizational 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the laws of France.

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 France.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor

Data exporter(s):

The data exporter and controller shall be Customer as defined in the Agreement, and data will be transferred by the data exporter to the data importer for purposes of fulfilling the HqO Service under the Agreement. By signing the Agreement, Customer agrees to these SCCs.

Data importer(s):

The data importer and processor shall be Vendor as defined in the Agreement, and data will be transferred by the data exporter to the data importer for purposes of fulfilling the HqO Service under the Agreement. By signing the Agreement, Vendor agrees to these SCCs.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Authorized Users (shall mean Customer, Company, Tenants and Tenant Users as defined in the Agreement)

Categories of personal data transferred

Customer or Tenants may submit Personal Data and or Customer Data to the Vendor, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

● First and last name

● Work Email Address

● Title

● Position

● Employer

● Temporary Access badge information

● Tenant status

● Location

● User ID

● Building ID

● Time stamp of activities using the HqO Mobile App and other HqO Service

● Usage data for the HqO Mobile App and other HqO Services (each as defined in the Agreement) ● Text, images, sound and other data entered by Authorized Users into the HqO Mobile App

● Technical support and other requests by Authorized Users

● Transactional data resulting from Authorized Users performing actions using features and functions of the HqO Mobile App and other HqO Services.

● Other Personal Data collected via the HqO Mobile App and other HqO Services as agreed to by the Customer from time to time.

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 specialized 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

The parties agree (for informational purposes only, and without creating additional obligations on either party or limiting the rights and obligations of either party otherwise existing), the following particulars of the Personal Data to be processed:

- Vendor will process Personal Data and Customer Data as necessary to perform the HqO Service and as further instructed by the Customer.

- Storage and other Processing necessary to provide, maintain and improve the HqO Service provided to Customer; and/or

- Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose(s) of the data transfer and further processing

Same as above.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The term of the Agreement and any period of transitional service provision subject to any other legal obligations of the Vendor.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Same as above and as necessary for the sub processor to assist Vendor in providing the HqO Service.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Same as Clause 13 above.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See https://www.hqo.com/security-practices/ for a description of HqO's technical and organizational measures. HqO will maintain technical and organizational measures that are at least as robust as those contained herein throughout the course of providing the HqO Service to Customer.

Schedule B

Subcontractor	Service Provided	Location of Processing
AWS	AWS is our hosting environment and our user database is stored in RDS (Amazon Aurora/MySQL). All user data is stored in AWS. All of our AWS services are hosted on a production VPC and are inaccessible to any traffic directly.	United States, EU
Stripe	Stripe is our payment processor. This affects any user who uses our Order Ahead functionality and enters their payment information into the Stripe SDK.	United States, EU
Braze	Braze will send push notifications and emails to users, and store a user's full name and email address.	United States, EU
LaunchDarkly	LaunchDarkly is used to A/B test features in our web dashboard (aka the "admin panel"). Access to the web dashboard is limited to a handful of customers per property. This is generally a very small subset of users. LaunchDarkly receives a user's full name and email address.	United States
Looker	Looker is a business intelligence software and big data analytics platform that we use to make sense of our usage analytics data.	United States, EU
Spreedly	Spreedly is our tokenizer solution for payment processing. This affects any	United States, EU

	users of our Order Ahead feature or other functions that involve payment functionality and enter their payment information. Spreedly actually stores their payment methods while the HqO app only stores an encrypted token that allows it to request payments when directed by the user.	
Snowflake	Snowflake is a data warehouse solution that is the central storage service underlying our data analytics platform.	United States, EU
Kafka	Kafla is a messaging middleware that connects the server-side of our applications in which user actions are captured to our data warehouse where these actions are stored for analysis and reporting. Kafka only stores data on a transient basis; long enough to ensure it was properly processed and received.	United States, EU