DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Appendices, ("**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, amends, and supplements 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 may collectively be referred to as 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:

A. **Definitions.** Any capitalized term used in this DPA that is not defined herein will have the same meaning set forth in the Agreement. 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) data 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.
8. "**Registered Authorized Users**" means users that have a User License.
9. "**User Data**" means data provided by Registered Authorized Users in connection with using the HqO Service.
10. "**User License**" means someone who has accepted the T&C in the app and is a user where a user is defined as 1. user of the app or web, 2. has a role, 3. not in a deactivated state, 4. in a non-deleted state."

B. 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.
   - 3.4 AI Restrictions. Vendor shall not use, or permit any subprocessors to use, any Personal Data or Customer Data as input to train, fine-tune, or otherwise feed any generative artificial intelligence system or large language model (LLM), whether internal or third-party, unless expressly authorized in writing by Customer.
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.**
    a. 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.
    b. 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 data 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.
    c. If Vendor receives any request or communication from a data subject that relates to the Processing of their 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.
    d. 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**.
    a. 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 Registered 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.

    b. 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.

    c. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area ("EEA") 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:

        i. 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.
        ii. Clause 9 of the Old EU SCCs specifies that United Kingdom law will govern the Old SCCs.
        iii. The content of Appendix 1 of the Old EU SCCs is set forth in Annex I of the New EU SCCs herein.
        iv. The content of Appendix 2 of the Old EU SCCs is set forth in the Annex II.

    d. 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 Act on Data Protection ("FADP") or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

e. 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:

a. 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.

b. 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.

c. 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).

d. 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.

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

f. 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.

g. 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.

C. 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 I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) 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] / [OPTION 2: Article 29(3) and (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].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data

received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least 60 days prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 60 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the

concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679/Articles 33, 36 to 38 Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

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 achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I 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.

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is transferred

Registered Authorized Users (shall mean Customer, Company, Tenants and Tenant Users as defined in the Agreement) means users that have a User License.

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 Registered Authorized Users into the HqO Mobile App
- Technical support and other requests by Registered Authorized Users
- Transactional data resulting from Registered 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 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

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 III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL 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 organization measures that are at least as robust as those contained herein throughout the course of providing the HqO Service to Customer.

HqO's solution is compliant with various data protection laws and regulations where our customers are residing, such as GDPR, CCPA, CPRA, The Dutch Telecommunications Act, and PIPEDA. View our Privacy Policy for more details.

HqO also leverages a number of third-party applications and services in support of the delivery of our solution to customers. We recognize that the company's information assets and vendor dependencies are critical to our continuing operations and delivery of services. As such, we have established a vendor management program that sets forth the requirements to be established and agreed upon when HqO engages with third parties or external vendors. For a complete list of HqO's sub-processors, please refer to our Data Processing Addendum document on our Legal Hub.

HqO maintains a comprehensive set of security policies and procedures which are communicated and accessible to all employees. We ask our employees during their onboarding and annually thereafter to read and understand these policies and procedures. We also plan, run, and continuously improve security awareness campaigns across the company to ensure all employees are aware of security best practices and how to best protect customers and other business information.

All policies and procedures that we have internally are bound to regular review at least annually. We also perform tests and compliance controls on all these areas to ensure that the measures are running effectively.

We host customer data on Amazon Web Services (AWS) infrastructure in the US East region data center located in Northern Virginia and the EU Central region data center located in Frankfurt, Germany. All primary instances of our infrastructure are replicated in real-time to secondary instances across multiple availability zones to ensure high availability service.

All data is encrypted during transmission and at rest. Backup snapshots of the database are captured at 5-minute intervals and retained for 30 days.

For ensuring the continuous security of our production environment, security vulnerability scanning is performed every 2 weeks using a third-party solution. Every year an external

party performs a penetration test on our applications (web and mobile) and infrastructure. All identified observations are tracked and resolved according to the policy and procedure previously defined.

HqO ISO Certification

ISO 27001

HqO is ISO 27001:2013 certified. The certification covers the ISMS supporting the confidentiality, integrity, and availability of customer data, supplier information, and HqO's internal data related to developing, operating, and planning a workplace experience platform environment.

HqO SOC 2

Certification SOC 2

HqO has obtained the SOC 2 Type II report by an examination of an independent third party. The report helps understand the controls HqO has established to support operations and compliance. The report is available upon request.

HqO STAR Certification

CSA Star Level 1

HqO has completed and regularly maintains the correctness of answers for security self-assessment (CAIQ v4.02) from Cloud Security Alliance (CSA). The completed questionnaire gives comprehensive information about the security practices that are in place at HqO.

ANNEX IV: LIST OF SUB-PROCESSORS

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 use our Order Ahead functionality and enter their payment information into the Stripe SDK.	United States, EU
Braze	Braze will send push notifications and emails to users, and stores a user’s full name and email	United States, EU

	address.	
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 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.	United States, EU
Snowflake	Snowflake is a data warehouse solution that is the central storage service underlying our data analytics platform.	United States, EU
Kafka	Kafka 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
Nexudus	Nexudus offers a web-based software-as-a-service white-label platform to manage your coworking and flex workspace.This affects any users who use our Nexudus functionality in scope of work.	EU, UK

Service Provider	**Data collected**	**Location of Data Processing**
Amazon Web Services	All application data	EU
Stripe	Payment information ● Credit card number ● Expiration date ● CVV2	US
Braze	● Email address	EU
LaunchDarkly	● Full Name ● Email address	US
Looker	Data analytics	EU
Spreedly	Payment information ● Credit card number ● Expiration date ● CVV2	US
Snowflake	Data analytics	EU
Kafka	Data analytics	EU
Nexudus	● E-mail ● Name ● Username and Password ● Application Data	EU, UK