HATHR DATA PROCESSING ADDENDUM

Updated: July 2025

This Hathr Data Processing Addendum (this "***DPA***") is hereby incorporated into the current version of the Customer Agreement (the "***Agreement***") by and between Customer (as defined in the Agreement) and Hathr, LLC., a Virginia limited liability company ("***Hathr***"), each a "***Party***" and collectively the "***Parties***."

This DPA applies to and takes precedence over the Agreement and any associated contractual document between the Parties, such as an order form or statement of work, to the extent of (but only to the extent of) any conflict or inconsistency between this DPA and the Agreement. Otherwise this DPA supplements and incorporates additional terms and conditions into the Agreement as and when it applies to the Platform provided under the Agreement.

All data processed, stored, or transmitted in connection with the Agreement and this DPA shall be restricted to the contiguous United States, defined as the 48 adjoining states and the District of Columbia, excluding Alaska, Hawaii, and all U.S. territories. This restriction applies to all data, including but not limited to personally identifiable information, protected health information, confidential information, sensitive agency data, and any associated metadata.

1. **Definitions**. For purposes of this DPA, the following terms are defined and shall be interpreted as set forth below. Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement or (if not defined therein) applicable Data Protection Laws:

"***Affiliates***" means a company, person or entity that is owned or controlled by, that owns or controls or is under common ownership or control with a Party. Ownership shall mean direct or indirect ownership of more than 50% of the equity in a company or entity, and control shall mean any power to appoint persons to the board of directors of a company or entity or to operate and manage same.

"***Controller***" means (i) the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; or (ii) a "***Business***" as that term is defined in the CCPA.

"***Data Protection Laws***" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, communications secrecy, breach notification, or the processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*. ("***CCPA***") and the General Data Protection Regulation, Regulation (EU) 2016/679 ("***GDPR***"). For the avoidance of doubt, if Hathr's processing activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.

"***Data Subject***" means an identified or identifiable natural person about whom Personal Data relates, including (i) an identified or identifiable natural person who is in the European Economic Area or whose rights are protected by the GDPR; or (ii) a "***Consumer***" as the term is defined in the CCPA.

"***Data Subject Rights***" means those rights identified in the GDPR and the CCPA granted to Data Subjects;

"***Personal Data***" includes "personal data," "personal information" and "personally identifiable information," and such terms shall have the same meaning as defined by the applicable Data Protection Laws.

"***Process***" and "***Processing***" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"***Processor***" means (i) a natural or legal person which processes personal data on behalf of the Controller; or (ii) a "***Service Provider***" as the term is defined in the CCPA.

"***Sale***" or "***Selling***" shall have the meaning defined in the CCPA.

"***Security Breach***" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data.

"***Security Measures***" means description of the technical and organizational security measures implemented by Hathr in its provision of the Platform to Customer as set out in Appendix 2 to Annex 1 of this DPA.

"***Sub-processor***" means (i) any processor engaged by the Processor or by any other Sub processor of the Processor who agrees to receive the Personal data exclusively intended for Processing activities to be carried out on behalf of the Controller after the transfer in accordance with Controller's instructions and in connection with the agreement for the provision of services to the Controller; or (ii) a Service Provider as defined in the CCPA;

"***Supervisory Authority***" means either (as applicable): (i) the United States Federal Government or (ii) the Commonwealth of Virginia, or, if applicable (ii) an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General.

"***United States Federal Government***" refers to the government of the United States of America, encompassing all its branches, departments and agencies.

2. **Scope and Purposes of Processing**.

(a) Hathr will Process all Personal Data solely to fulfill its obligations to Customer under the Agreement and this DPA and on Customer's behalf, and for no other purposes, unless required to do otherwise by Data Protection Laws to which Hathr is subject. In such case, Hathr will inform Customer of that legal requirement before Processing, unless that law prohibits Customer from providing such information to Hathr. With regard to the Processing of Personal Data, Hathr will act as a Processor and Customer on which behalf the Personal Data is processed

will act as Controller. Each Party will fully comply with the obligations that apply to it under the Data Protection Laws. The Personal Data shall remain at all times the Controller's property.

(b) Without limiting the foregoing, Customer directs Hathr to Process Personal Data in accordance with Customer's written instructions, as may be provided by Customer to Hathr from time to time and in the following manner.

(i) Subject matter, nature, and purpose of Processing: Hathr will Process data solely to provide Customer with the Platform (including access to the Platform) (collectively, the "***Platform***") and to fulfill its purposes under the Agreement, which may include any lawful processing or business purposes as provided for under applicable Data Protection Laws. The Processing by Hathr shall consist of all permitted processing operations under the Agreement necessary to provide the Platform.

(ii) Anticipated duration of Processing: For the term of the Agreement or to the extent that Hathr continues to Process Personal Data (including for internal tax and audit purposes), whichever is longer.

(iii) Categories of Personal Data typically subject to Processing: All types of Personal Data including special categories of data, as that term is defined and permitted under applicable Data Protection Laws.

(iv) Typical categories of Data Subjects: All types of Data Subjects.

(c) Hathr will immediately inform Customer if, in Hathr's opinion, an instruction from Customer infringes Data Protection Laws.

(d) Hathr will not:

(i) Sell Personal Data as defined in the CCPA.

(ii) Process Personal Data for any purpose other than for the specific purposes set forth herein. For the avoidance of doubt, Hathr will not Process Personal Data outside of the direct business relationship between Customer and Hathr or for a commercial purpose other than providing the Platform.

(iii) Attempt to link, identify or otherwise create a relationship between Personal Data and non-Personal Data or any other data except as authorized under the Agreement or as necessary to provide the Platform without the express authorization of Customer.

(e) For GDPR purposes, information that has been anonymized is not Personal Data. For CCPA purposes, information that has been de-identified is not Personal Data and Hathr may de-identify Personal Data only if it:

(i) Has implemented technical safeguards that prohibit reidentification of the Data Subject to whom the information may pertain;

(ii) Has implemented business processes that specifically prohibit reidentification of the information;

(iii) Has implemented business processes to prevent inadvertent release of deidentified information; and

(iv) Makes no attempt to reidentify the information.

3. **Compliance with Data Protection Laws**.

(a) Hathr will only Process Personal Data as set forth in this DPA and in compliance with Data Protection Laws.

(b) Hathr hereby certifies that it understands its restrictions and obligations set forth in this DPA and will comply with them.

4. **Personal Data Processing Requirements**. Hathr will:

(a) Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(b) Upon written request of Customer, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their representatives) for exercising their Data Subject Rights (such as rights to access or delete Personal Data).

(c) Promptly notify Customer of (i) any third-party or Data Subject requests or complaints regarding the Processing of Personal Data; or (ii) any Supervisory Authority or Data Subject requests for access to or information about Hathr's Processing of Personal Data on Customer's behalf, unless prohibited by Data Protection Laws. If Hathr receives a third-party, Data Subject, or Supervisory Authority request, Hathr will await written instructions from Customer on how, if at all, to assist in responding to the request. Hathr will provide Customer with reasonable cooperation and assistance in relation to any such request.

(d) To the extent that Hathr believes or becomes aware that its Processing or the Processing proposed by Customer of Personal Data is likely to result in a high risk (as defined in the applicable Data Protection Laws) with regard to the rights and freedoms of Data Subjects, it shall promptly inform the Customer and cooperate, at its own expense, as requested by the Customer to enable it to respond and comply with applicable Data Protection Laws, including providing reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of the Processing or proposed Processing of Personal Data.

(e) Provide reasonable assistance to and cooperation with Customer for Customer's consultation with any Supervisory Authority in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Hathr under Data Protection Laws to consult with a Supervisory Authority in relation to Hathr's Processing or proposed Processing of Personal Data.

5. **Data Security**. Hathr will implement appropriate administrative, technical, physical and organizational measures prior to and during Processing of any Personal Data to protect the security, confidentiality and integrity of the data and to protect the data against any form of Security Breach. Hathr shall ensure a level of security appropriate to the risks presented by the processing of Personal Data and the nature of such Personal Data. Such measures shall include, as appropriate:

(a) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(b) The ability to restore the availability and access to the Personal Data in timely manner in the event of a physical or technical security incident;

(c) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

At a minimum, such measures shall include the Security Measures which meet or exceed relevant industry practice. As of the Effective Date of the Agreement, Hathr has implemented the Security Measures. Hathr may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Platform.

6. **Duty to Notify and Cooperate**. Hathr will promptly notify Customer and/or fully cooperate with Customer:

(a) If after a reasonable investigation, Hathr becomes aware of any Security Breach relating to its or its Sub-processor's use or Processing of Personal Data. In such case, Hathr shall promptly inform the Customer of the Security Breach without undue delay and shall provide all such timely information and cooperation as the Customer may reasonably require including in order for the Customer to fulfil its data breach reporting obligations under and in accordance with applicable Data Protection Laws. Hathr shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Breach that are under its reasonable control and shall keep the Customer up-to-date about all developments in connection with the Security Breach. Hathr shall also take all reasonable, necessary and appropriate steps to remedy any non-compliance with Data Protection Laws or cease further Processing of Personal Data, and the Controller may immediately terminate Hathr's access to Personal Data or take any other necessary action as determined in its sole discretion;

(b) To enable the Customer to comply with its obligations with regard to the security of the Processing of Personal Data, taking into account the nature of the Processing and the information available to Hathr;

(c) Upon the Customer's request, to make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the Processing of the Personal Data available to the Customer in order to allow the Customer to demonstrate compliance with its obligations laid down in applicable Data Protection Laws. In particular, the Customer or a third party appointed by the Customer (the "***Auditor***") may enter Hathr's premises or the location where Personal Data is Processed, on reasonable notice during regular business hours and subject to appropriate confidentiality obligations, to verify Hathr's compliance hereunder. The identity of the Auditor and the scope, timing and duration of the audit shall be separately agreed upon between the Parties. The Customer or the Auditor may also inspect, audit and review (but not remove sensitive network design or configuration data) any relevant records, processes and systems to verify compliance with the applicable Data Protection Laws and this DPA. The Customer shall take all reasonable measures to prevent unnecessary disruption to Hathr's and/or its Sub-processor's operations. The audits will be at Customer's expense and Customer will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period and with at least thirty days' prior written notice, except (i) if and when required by instruction of a competent Supervisory Authority or (ii) the Customer believes a further audit is necessary due to a Security Breach by Hathr.

7. **Subcontractors**.

(a) Customer acknowledges and agrees that Hathr may use Hathr affiliates and other subcontractors to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Hathr's Hosting Provider is identified in the Agreement and Customer will be notified of other Sub-processors in Annex 1 or amendments thereto or otherwise in writing upon Customer's request.

(b) Where Hathr sub-contracts any of its rights or obligations concerning Personal Data, including to any affiliate or Sub-processor, Hathr will (i) take steps to select and retain subcontractors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Protection Laws; and (ii) enter into a written agreement with each subcontractor that imposes obligations on the subcontractor that are no less restrictive than those imposed on Hathr under this DPA.

(c) If Hathr provides notice to Customer of a proposed change to subcontractors or Sub-processors, Customer shall raise any objection to the appointment thereof within ten (10) days of Hathr's notice to Customer. In the event Customer objects to a new subcontractor or Sub-processor, Hathr will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer' use of the services by the objected-to subcontractor or Sub-processor.

8. **Data Transfers**. In the event that Customer transfers Personal Data of Data Subjects located in the European Economic Area to Hathr in the United States, Hathr agrees to be bound by the standard contractual clauses for the transfer of personal data to processors established in third countries ("***Model Clauses***") attached hereto as Annex 1. In case of conflict between the Model Clauses and this DPA, the Model Clauses will prevail. The Model Clauses shall not apply where Hathr Processes Personal Data (i) in a country that the European Commission has decided provides adequate protection for Personal Data and (ii) shall not apply to any Processing by Hathr of Personal Data that is not subject to GDPR.

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Protection Laws, Hathr will return to Customer and/or securely destroy (with proof of such destruction) all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Protection Laws, Hathr will inform Customer if it is not able to return or delete any Personal Data. Any remaining Personal Data which is not deleted or effectively anonymized will be unavailable for any further Processing except to the extent required by applicable laws, including but not limited to Data Protection Laws.

10. **Governing Law, Indemnification, Limitation of Liability**. Except as required by the Model Clauses for such Personal Data as and when subject thereto, the governing law, indemnification obligations and limitations of damages and liability arising out of or related to this DPA are subject to the provisions applicable thereto in the Agreement.

11. **Term**. The effective date of this DPA shall be the date on which the term of the Agreement commences. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Hathr or its Sub-Processors Process the Personal Data subject hereto or as otherwise agreed by the Parties in writing.

ANNEX I: STANDARD CONTRACTUAL CLAUSES (MODEL CLAUSES)

Annex 1

To HATHR Data Processing Agreement

Standard Contractual Clauses (Controller-to-Processor Transfers)

For the purposes of Article 26(2) of General Data Protection Regulation (EU) 2016/679 ("GDPR") for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection:

The entity identified as "Customer" in the DPA (the "data exporter**"**) and the entity identified as "HATHR" (the "data importer") in the Hathr Data Processing Agreement ("DPA") each a "Party" and together "the Parties:"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

SECTION I

CLAUSE 1

Purpose and scope

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

(b) The Parties:

(i) 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.

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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

CLAUSE 4

Interpretation

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

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

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 organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information

for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

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

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

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

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

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

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

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

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

CLAUSE 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform

the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*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.

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

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

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

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

CLAUSE 10

Data subject rights

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

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

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

CLAUSE 11

Redress

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

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

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

(i) lodge a complaint with the applicable Supervisory Authority in the , competent Supervisory Authority jurisdiction pursuant to Clause 13;

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

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

(e) The data importer shall abide by a decision that is binding under the laws of the United States Federal Government, the Commonwealth of Virginia, and any other applicable US state

(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) In no event will either party be liable for any consequential, indirect, exemplary, special, or incidental damages, including any lost data and lost profits arising from or relating to this Agreement even if advised of the possibility of such damages either party's total cumulative liability in connection to this Agreement, whether in contract, tort, or otherwise, will not exceed the total price under the applicable PO.

(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, but will not exceed the total price under the applicable PO.

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

CLAUSE 13

Supervision

(a) The Supervisory Authority is the jurisdiction in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

CLAUSE 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the United States Federal Government or a specific state in which the Clauses apply adopts a material decision that covers the transfer of personal data or (ii) the European Commission adopts a material 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 laws of the United States Federal Government first, followed by the laws of the Commonwealth of Virginia, and, where neither provides clear guidance, by the laws of another relevant U.S. state consistent with federal and Virginia law. If none of the foregoing is applicable, the these Clauses shall be governed by an applicable EU Member State (without regard to its conflicts of law's provisions) with regard to its validity, construction, interpretation, performance, and enforcement. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State identified by Hathr. PARTIES HEREBY WAIVE TRIAL BY JURY WITH RESPECT TO ALL CAUSES OF ACTIONS ARISING UNDER THIS AGREEMENT. Nothing in this Section precludes a party from seeking immediate court ordered injunctive relief from any court of competent jurisdiction upon reasonable belief of immediate harm. If any legal action is

instituted to enforce this Agreement, the prevailing party is entitled to recover reasonable attorneys' fees and costs from the other party.

CLAUSE 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved first by the state or federal courts of the Commonwealth of Virginia or, if applicable, by an EU Member State.

(b) If the dispute must be resolved by an EU Member States, the Parties agree that those shall be the courts of the Member State identified by Hathr.

(c) If the dispute must be resolved by an EU Member State, 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 in the Commonwealth of Virginia, or if not applicable, by the court of the Member State identified by Hathr.

Appendix 1

to HATHR DPA Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. By you agreeing to the Agreement, the parties will be deemed to have signed this Appendix 1.

Data exporter

The data exporter is the entity identified as "Customer" in the DPA.

Data importer

The data importer is the entity identified as "Hathr" in the DPA.

Data Subjects

Data subjects include the data exporter's personnel, representatives, contractors, partners, vendors, and persons of interest.

Categories of data

The Personal Data which is Processed by the data importer through the data exporter's use of the Platform as described in the Agreement. The data exporter determines the types of data per each Service used.

Processing operations

The Personal Data transferred will be subject to the processing activities required for performance of the Platform by data importer pursuant to the Agreement between them. Data importer may use Sub-processors in connection with its Processing activities for data exporter.

Appendix 2

To Hathr DPA Standard Contractual Clauses

Security Measures

Description of the technical and organizational security measures implemented by HATHR in its provision of the Platform to Customer under the Agreement:

1. Security.

1.1. Security Management System.

(a) **Organization.** Processor designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.

(b) **Policies.** The data importer's executive management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Personal Data. These policies are updated at least once annually.

(c) **Assessments.** Processor engages a reputable independent third-party to perform risk assessments of all systems containing Personal Data at least once annually.

(d) **Risk Treatment.** Processor maintains a formal and effective risk treatment program to identify and protect against potential threats to the security, integrity or confidentiality of Personal Data.

(e) **Sub-processor Management.** Processor maintains a formal and effective sub-processor management program.

(f) **Incident Management.** Processor reviews security incidents regularly, including effective determination of root cause and corrective action.

2. Personnel Security.

2.1. Processor personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Processor conducts reasonably appropriate criminal background checks on any employees who will have access to Personal Data under this Agreement, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

2.2. Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Personal Data at all times. Personnel must acknowledge receipt of, and compliance with, Processor's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Personal data are required to complete additional requirements appropriate to their role (e.g., certifications). Processor's personnel will not process Personal data without authorization.

3. Access and Site Controls.

3.1 Hosting Provider Security Measures. Description of the technical organizational security measures implemented by the Sub-processor processing Personal Data, which Processor is subject to in all respects, is included in the data processing addendum linked to below. The security standards in the Sub-processor's data processing addendum provided in the link below are incorporated by reference, as amended from time to time by the Sub-processor or as replaced by a substitute Sub-processor, subject to the obligations of Processor in the Agreement when replacing Sub-processors:

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

3.2. Access Control.

(a) **Access Management.** Processor maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Personal Data to limit access to Personal Data and systems storing, accessing or transmitting Personal Data to properly authorized persons having a need for such access. Access reviews are conducted periodically (no less than annually) to ensure that only those personnel with access to Personal Data still require it.

(b) **Infrastructure Security Personnel.** Processor has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Processor's infrastructure security personnel are responsible for the ongoing monitoring of Processor's security infrastructure, the review of the Platform, and for responding to security incidents.

(c) **Access Control and Privilege Management.** Processor's and Client's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Platform. Each application checks credentials in order to allow the display of data to an authorized user or administrator.

(d) **Internal Data Access Processes and Policies – Access Policy.** Processor's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. Processor designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. Processor employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Processor requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Processor's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity.

4. Data Center & Network Security.

4.1 Data Centers.

(a) **Server Operating Systems.** Processor's servers are customized for the application environment and the servers have been hardened for the security of the Platform

(b) **Disaster Recovery.** Processor replicates data over multiple systems to help to protect against accidental destruction or loss. Processor has designed and regularly plans and tests its disaster recovery programs.

(c) **Security Logs.** Processor's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, Processor's systems.

(d) **Vulnerability Management.** Processor performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

4.2. Networks & Transmission.

(a) **Data Transmission.** Transmissions between data centers are designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Processor transfers data via Internet standard protocols.

(b) **External Attack Surface.** Processor employs multiple layers of network devices and intrusion detection to protect its external attack surface. Processor considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

(c) **Intrusion Detection.** Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Processor intrusion detection involves:

(i) Tightly controlling the size and make-up of Processor's attack surface through preventative measures; and

(ii) Employing intelligent detection controls at data entry points.

(d) **Incident Response.** Processor maintains incident management policies and procedures, including detailed security incident escalation procedures. Processor monitors a variety of communication channels for security incidents, and Processor's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.

(e) **Encryption Technologies.** Processor makes HTTPS encryption (also referred to as SSL or TLS) available.