vFairs Global Data Processing Addendum

This Data Processing Addendum (“Addendum” or "DPA") supplements the vFairs LLC Master Subscription Agreement (the “Agreement”) entered into by and between:

[Customer signing this Addendum] (“Customer” or "Client")

and

vFairs LLC (“Company”).

This Addendum incorporates the terms of the Agreement, and any terms not defined in this Addendum shall have the meaning set forth in the Agreement or if not therein defined the definition from the applicable Data Protection Law.

WHEREAS,

(A) The Customer acts as a Data Controller or a processor to a Data Controller.

(B) The Customer wishes to contract certain Services, which imply the processing of personal data, to the Company (Data Processor).

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and any applicable security and privacy laws and regulations, including, without limitation, the CCPA and the EU General Data Protection Regulation 2016/679 (“GDPR”).

(D) The Parties wish to lay down their rights and obligations.

This DPA consists of (a) the main body of the DPA; (b) the Standard Contractual Clauses (Module 2: Controller to Processor and Module 3: Processor to Processor) including Annex I, II and III.

Definitions

1.1 “Customer Account Data” means personal data that relates to Customer’s relationship with Company, including the names or contact information of individuals authorized by Customer to access Customer’s account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.2 “Customer Usage Data” means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.3 "Consumer" in the text of CCPA, is a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations.

1.4 "Data Center" is a facility that provides shared access to applications and data using a complex network, compute, and storage infrastructure

1.5 "Data Exporter" means Customer.

1.6 "Data Importer" means Company.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the Swiss Federal Act on Data Protection, (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); (v) the UK Data Protection Act 2018; and (vi) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.8 "Data Subject" a natural person whose personal data is processed by a data controller or processor.

1.9 "Personal Data Breach" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.10 "Processing" any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "Personal Data" any information relating to an identified or identifiable natural person ('data subject'); 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.

1.12 "Restricted Transfer" means (i) a transfer of Controller Personal Data from Controller to Processor; or (ii) an onward transfer of Controller Personal Data from a Processor to a Sub Processor, or between two establishments of Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

1.13 "Standard Contractual Clauses" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

1.14 "Subprocessor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in Annex III or (2) subsequently authorized under Clause 9 of the SCCs included in this Addendum.

1.15 "Services" shall have the meaning set forth in the Agreement.

2.1. Processing of Personal Data

The parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Data Controller or a processor to the Data Controller, and vFairs is the Data Processor.

2.2. vFairs will and will ensure that Subprocessors will Process Client Personal Data only on Client's documented instructions, or where Processing is required by applicable laws to which vFairs or subprocessors are subject; in the latter case, vFairs will notify the Client of the legal requirement before processing, unless the law prohibits such notification.

2.3. Client instructs vFairs (and authorizes vFairs to instruct each Subprocessor) to, as reasonably necessary for the provision of the Services: (a) Process Client Personal Data; (b) transfer Client Personal Data to any country or territory provided such complies with Section 10 (Cross-border Transfers) below; and (c) engage any Subprocessors, provided such complies with Section 9 (Subprocessing) below. If requested by Client and set forth in an Agreement, vFairs will store Client Personal Data in a Data Center located in the European Union. Client agrees that technical limitations may apply to the use of a Data Center in the European Union as further specified in the applicable Agreement or as otherwise communicated to Client.

2.4. Pursuant to, and as required under the CCPA, vFairs will process Client Personal Data to the extent necessary to provide the Services described in the Agreement and only for the purposes as instructed by Client in a manner consistent with this Addendum. vFairs will not retain, use, or disclose such Client Personal Data for any purpose other than to perform the Services, which for the avoidance of doubt prohibits vFairs from retaining, using, or disclosing Client Personal Data outside of the direct business relationship with Client or for any other commercial purpose. vFairs will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise

communicate such Client Personal Data to any third party for monetary or other valuable consideration. vFairs certifies that that it understands the restrictions set out in this Section 2.4 and will comply with them. Client agrees that vFairs may de-identify or aggregate Client Personal Data and other data related to the Services to render it Anonymous Data, which may then be used for the purposes of operating and improving vFairs's services and operations, and other research, analytics and related purposes. vFairs may maintain Anonymous Data as part of its own records and information, and such data shall no longer be subject to the Agreement or this Addendum. "Anonymous Data" means data that has been de-identified and/or aggregated with other data to such an extent that Client data is no longer identifiable, and individuals are no longer identified, identifiable, linked or linkable, or otherwise ascertainable by reference to or combination with other datasets.

2.5. Client agrees that (a) Client's submission of Client Personal Data and instructions for the Processing of Personal Data will comply with Data Protection Laws and Client will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section (Processing of Personal Data) (b) Client will, in the use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws; and (c) Client will provide any required notices to and obtain any required consents from Data Subjects related to the Processing of Client Personal Data as contemplated in this Addendum and the Agreement, or as otherwise instructed by Client.

2.6. Annex 1 to this Addendum sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, and the categories of Personal Data and Data Subjects, as required by Article 28(3) of the GDPR. Either of the parties may make reasonable amendments to Annex 1 as they reasonably consider necessary to meet the requirements of Article 28(3) of the GDPR by providing the other party with an updated or an additional Annex 1.

3. vFairs Personnel
vFairs will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Client Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

4. Security
vFairs will implement appropriate technical and organizational measures, as set forth in Annex 2 (Technical and Organizational Measures), that are designed to provide a level of security appropriate to the risks presented by the Processing of Client Personal Data. In assessing the appropriate level of security, vFairs will take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

5. Personal Data Breach
vFairs will notify Client without undue delay if it discovers a Personal Data Breach involving Client Personal Data and will provide information (as available) to assist Client to meet any obligations to report a Personal Data Breach under the Data Protection Laws. vFairs will co-operate with Client and take such reasonable steps as are agreed in good faith by the parties to

assist in the investigation, mitigation and remediation of each Data Breach. To the extent that Client is responsible for a Personal Data Breach Client will reimburse vFairs for all costs reasonably and properly incurred by vFairs performing its obligations under this Section (including internal costs and third-party costs including legal fees).

6. Data Subject and Consumer Rights
vFairs will promptly notify Client if it receives a request from a Data Subject or Consumer entitled to exercise a request under applicable law regarding Client Personal Data as it pertains to that Data Subject or Consumer. Upon request, vFairs will provide Client with reasonable assistance as necessary to Client's fulfilment of its obligations under applicable laws to respond to such requests relating to their Personal Data. Taking into account the nature of the Processing, such assistance will include, where practicable, implementation of reasonable and appropriate technical and organizational measures to allow Client to respond effectively to such requests.

7. Data Protection Impact Assessment and Prior Consultation
Upon request and subject to the nature of the relevant Processing by and information available to vFairs, vFairs will provide reasonable assistance to Client with any data protection impact assessments and any prior consultations to any Supervisory Authority, which are required under applicable Data Protection Law. Client will reimburse vFairs in full for all costs reasonably and properly incurred by vFairs in performing its obligations under this Section (including internal costs and third-party costs including legal fees).

8. Audit Rights
8.1 Upon Client's written request, vFairs will make available to Client information reasonably necessary to demonstrate vFairs compliance with this Addendum, and will allow for and contribute to inspections by a qualified, independent third-party auditor appointed by Client, in relation to the Processing of Client Personal Data by vFairs or its Sub processors.

8.2 Client will give vFairs reasonable notice of any audit or inspection to be conducted under this Section and will (and ensure that each of its mandated auditors will) take all reasonable steps to avoid causing any damage, injury or disruption to the premises, equipment, personnel and business of vFairs or any Subprocessor during the course of such an audit. Except as otherwise required by applicable law or a relevant Supervisory Authority, any audit or inspection will be conducted within normal business hours no more than once in any calendar year. Client will reimburse vFairs in full for all costs reasonably and properly incurred by vFairs performing its obligations under this Section (including internal costs, third party costs including legal fees, and costs incurred by vFairs with respect to audits of other Subprocessors). Any information obtained under this Section will be kept confidential and not disclosed to any person without the express consent of vFairs, and Client will ensure that any auditor, agent, personnel or other person or entity that participates in such audit is subject to appropriate written confidentiality obligations.

9. Sub processing
9.1 Client authorizes vFairs to appoint (and permit each Subprocessor appointed in accordance with this Section to appoint) Subprocessors. Client expressly agrees that vFairs may continue to use those other Subprocessors already engaged by vFairs as of the date of this Addendum.

9.2 The parties will work in good faith to resolve Client's objections to the appointment of any Subprocessors. During this time, there may be an impact to the provision of the Services; Client agrees that vFairs is not liable for any such impact. If the parties are unable to resolve Client's objection within 90 days, Client may terminate without penalty the portion of the Agreement pertaining to the Services that vFairs states it cannot provide without the use of the objected-to Subprocessor, and vFairs will refund Client any prepaid but unused amounts for such portion; otherwise the Agreement shall remain in full force and effect.

9.3 With respect to each Subprocessor, vFairs will: (a) exercise commercially reasonable care in the assessment, appointment and oversight of the relevant Processing activities of Subprocessors; (b) include terms in the contract between vFairs and each Subprocessor which offer an equivalent level of protection for Client Personal Data as those set out in this Addendum, taking into account the nature of the services performed by the Subprocessor; (c) if the arrangement involves a Restricted Transfer of Client Personal Data vFairs will ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between vFairs and the Subprocessor; and (d) remain liable to the Client for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of Client Personal Data as if such failure was its own.

10. Cross-border Transfers

Client, as data exporter, and vFairs, as a data importer, hereby execute the Standard Contractual Clauses attached, which shall apply to the Client Personal Data and take effect in the event of a Restricted Transfer of Client Personal Data. With respect to the Client Personal Data subject to Data Protection Laws other than those of the EEA or the United Kingdom, that apply to Restricted Transfers, in the Standard Contractual Clauses, the terms "Member State" and "State" are replaced throughout by the word "jurisdiction," "supervisory authority" will mean the relevant data protection regulator or other government body with authority to enforce Data Protection Laws, and references to "applicable data protection laws" and "Directive 95/46/EC" shall be replaced with the "applicable Data Protection Laws" as defined herein.

11. Deletion or Return of Personal Data

Upon the termination or expiration of the Agreement (unless continued Processing is subject to a new or amended agreement) and to the extent not prohibited by applicable law, vFairs will within 90 days cease Processing and delete or return the Client Personal Data. If Client does not inform vFairs of its choice of either return or deletion of such Client Personal Data at least 30 days after termination or expiration of the Agreement, then Client will be deemed to have chosen deletion. The parties agree that vFairs is not required to return or delete any Anonymous Data at the conclusion of the Agreement.

12. Limitation of Liability

The aggregate liability of vFairs arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability in the Agreement. To the extent permitted by Data Protection Law, the limitations of liability between Company and Client shall apply to liability between Company and Client in the Standard Contractual Clauses, provided that this provision shall not vary liability to a Data Subject under the Standard Contractual Clauses.

13. Miscellaneous.
13.1 Interpretation. The terms and conditions of this DPA shall be subject to the terms and conditions of the Agreement, provided that, in the event of a direct conflict concerning data protection between the terms and conditions of this DPA and the Agreement, this DPA shall control.

13.2 Modifications. No alteration, amendment, or modification of this DPA will be valid unless in writing and signed by an authorized representative of both parties.

13.3 Invalidity. Should any provision of this DPA be found invalid or unenforceable pursuant to any applicable law, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the DPA will continue in effect.

13.4 Duration. This DPA will become legally binding upon the effective date of the Agreement or upon the date that the last party signs this DPA if it is completed after the effective date of the Agreement. The DPA shall remain in effect until the termination of the Agreement.

13.5 Survival. The respective rights and obligations of the parties under this DPA shall survive termination of the DPA to the extent necessary to fulfill their purposes.

13.6 No Third Party Beneficiaries - Except as expressly required by Data Protection Laws for a Data Subject in the Standard Contractual Clauses, no provisions of this Addendum is intended to benefit any person or entity not a party to this Addendum, nor shall any person or entity not a party to this Addendum have any right to seek to enforce or recover any right or remedy with respect hereto.

IN WITNESS WHEREOF, the parties hereto
have executed this DPA.

COMPANY:	CLIENT:
By:_____	By:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____
Dated:_____	Dated:_____

STANDARD CONTRACTUAL CLAUSES

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

(b) The Parties:

[Customer Name], an entity organised under the laws of [ ], with a business address at [ ]

And

vFairs LLC an entity organised under the laws of State of Delaware with a business address at 1510 Randolph St, Ste 208, Carrollton, TX 75006

(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.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8 – 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.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

MODULE TWO: Transfer controller to processor

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[2] (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.

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

(b) 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.

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter(5)

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725. .

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union(6)

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

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

MODULE TWO: Transfer Controller to processor

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data

exporter with the information necessary to enable the data exporter to exercise its right to object.

:(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer 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.

MODULE THREE: Transfer processor to processor

GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.(9)

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

MODULE TWO: Transfer controller to processor

(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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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

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.
[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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:

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

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

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

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

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

Clause 12

Liability

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

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

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

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

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

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

Clause 13

Supervision

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising

access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(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).

---

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

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of EU Member State in which the data exporter is established.

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

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

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

Processing as necessary for virtual events of Customer on the vFairs platform and any other services in accordance with the DPA and the Service Agreement

_____

_____

Signature and date: _____

Role: Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ___vFairs LLC_____

Address: 1510 Randolph St Ste 208, Carrollton, TX 75006, USA_____

Contact person's name, position and contact details: _____

Rizwan Tanveer, Data Protection Officer, privacy@vfairs.com

Activities relevant to the data transferred under these Clauses:

Processing as necessary for virtual events of Customer on the vFairs platform and any other services in accordance with the DPA and the Service Agreement

Signature and date: _____

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Virtual event participants, exhibitors, speakers and other data subjects as necessary for the services provided to Customer.

Categories of personal data transferred

Company processes Personal Data contained in Customer Account Data, Customer Usage Data, and any Personal Data provided by Customer or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this Addendum. Categories of Personal Data may include first name, last name, email ID, IP address etc.

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.

Not Applicable

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

During the term of the Agreement on a periodic basis and/or at the discretion of the Customer.

Nature of the processing

Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum.

Purpose(s) of the data transfer and further processing

Processing as necessary for virtual events of Customer on the Company platform and any other services in accordance with the DPA and the Service Agreement

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

Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Customer Account Data and Customer Usage Data will be processed and stored as set forth in Company's privacy policy.

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

Refer to Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

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

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13.

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Company has deployed methods and protocols for secure transmission of confidential or sensitive information over public networks. Databases housing personal customer data are encrypted at rest. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Company's customer agreements contain strict confidentiality obligations. Additionally, Company requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Segment's customer agreements. Company has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily and weekly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Company has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Company uses secure access protocols and processes and follows industry standard practices for authentication, including Multifactor Authentication and Single Sign On (SSO). All production access requires the use of two-factor authentication, and network infrastructure is configured to vendor and industry practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	Company has deployed methods and protocols for secure transmission of confidential or sensitive information over public networks. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)

Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data.
Measures for ensuring physical security of locations at which personal data are processed	We use AWS to host our infrastructure. AWS manages the physical security of its data centers with state-of-the-art controls. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Company monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Company adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Company maintains a risk-based information security governance program. The framework for Company's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assurance of processes and products	Company undergoes annual SOC 2 Type II audit.
Measures for ensuring data minimisation	Company's Customers unilaterally determine what Customer PII Data they route through the Services. As such, Company operates on a shared responsibility model. Company gives Customers control over exactly what PII data enters the platform. Additionally, Company has built in self-service functionality to the Services that allows Customers to delete and suppress PII at their discretion.
Measures for ensuring data quality	Company has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design using GraphQL and strong typing to enforce a strict contract between official clients and API resolvers. Company applies these measures across the board, both to ensure the quality of any Usage Data that Company collects and to ensure that the Company Platform is operating within expected parameters.

	Company ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.
Measures for ensuring limited data retention	Company Customers determine what Customer Data they route through the Services. As such, Company operates on a shared responsibility model. If a Customer is unable to delete Customer PII Data via the self-services functionality of the Services, then the Company deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law. All Customer Data is deleted from the Services following service termination.
Measures for ensuring accountability	Company has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Security Incidents involving Personal Data, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, the Company conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	All PII in the Services may be deleted by the Customer or at the Customer's request. PII is incidental to the Company's Services. Based on Privacy by Design and Data Minimization principles, Company severely limits the instances of PII collection and processing within the Services. Most use cases for porting PII from Company are not applicable. However, Company will respond to all requests for data porting in order to address Customer needs.
Technical and organizational measures of sub-processors	The Company enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Addendum.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

The Company enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. *Name: Amazon AWS, USA*

Description of processing: Infrastructure Host

2. *Name: Zoom, USA*

Description of processing: Live Webinar Host

3. *Name: Pubnub, USA*

Description of processing: Integrated Chat Platform

4. *Name: Vimeo, USA*

Description of processing: Video Hosting

5. *Name: Whereby, Norway*

Description of processing: Video Conferencing