VISUAL LEASE

**Visual Lease: Data Processing Addendum**

This Data Processing Addendum, including its Attachments, Exhibits, and Annexes ("Addendum"), is incorporated into and forms part of the Order Form for Visual Lease ("VL") Services (or other form of agreement between the Parties, as applicable) (the "Agreement") by and between VL and Client (collectively, the "Parties"). This Addendum sets forth the terms and conditions relating to compliance with Privacy Laws (as defined below) in connection with the Services to be rendered by VL to Client pursuant to the Agreement.

Whereas, VL (1) provides Services to Client pursuant to the Agreement and (2) Processes, on behalf of Client, Personal Information that is necessary to perform the Services under the Agreement; and

Whereas, Client requires that VL preserve and maintain the privacy, confidentiality, and security of such Personal Information.

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement, and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Client and VL agree as follows:

## 1. Definitions

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Information.

"**Data Subject**" means an identified or identifiable natural person to which the Personal Information pertains.

"**European Data Protection Laws**" means applicable European Union ("EU"), European Economic Area ("EEA"), or national laws and regulations (including laws and regulations of the United Kingdom ("UK") or Switzerland) relating to the privacy, confidentiality, security, or protection of Personal Information, including the EU General Data Protection Regulation 2016/679 ("GDPR") and laws or regulations implementing or supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive") and laws or regulations implementing or supplementing the e-Privacy Directive; the GDPR as incorporated into UK law ("UK GDPR") and the Data Protection Act 2018; and the Swiss Federal Act on Data Protection ("Swiss DPA").

"**Information Security Incident**" means any actual or reasonably suspected unauthorized or accidental access to or loss, use, disclosure, modification, destruction, acquisition, or Processing of any Personal Information.

"**Instructions**" means this Addendum and any further written agreement or documentation through which Client instructs VL to perform specific Processing of Personal Information.

"**Personal Information**" means information that identifies, links to, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, that may be (i) Processed at any time by VL in anticipation of, in connection with or incidental to the performance of the Agreement or (ii) derived by VL from such information.

"**Privacy Laws**" means applicable international, federal, state, and local laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality or security of Personal Information, including without limitation, European Data Protection Laws, and the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020), Cal. Civil Code § 1798.100 et seq., and its implementing regulations (collectively, "CCPA")

"**Process**" (and its derivatives) means any operation or set of operations performed, whether or not by automated means, on Personal Information, such as creating, collecting, procuring, obtaining, retaining, accessing, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, transmitting, aligning, combining, restricting, erasing, anonymizing, deleting, or destroying the data.

"**Processor**" means any person or entity that Processes Personal Information on behalf of a Controller.

"**Sub-Processor**" means any entity engaged by VL (or any further Sub-Processor), including affiliates of VL, to Process Personal Information on behalf and under the authority of Client.

"**Business**", "**Business Purpose**", "**Deidentified**" (and its derivatives), "**Sell**" (and its derivatives), "**Share**" (and its derivatives), "**Service Provider**", and any other capitalized term used but not defined herein shall have the meaning ascribed to it in the applicable Privacy Laws, except that the definition of Personal Information set forth in this Addendum shall control in any and all cases.

## 2. Roles and Responsibilities of the Parties

2.1 The Parties acknowledge and agree that Client is acting as a Business and Controller, and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Information Processed under this Addendum, and VL is acting as a Service Provider and Processor on behalf and under the Instructions of Client. The Personal Information that Client discloses to VL is provided to VL for the limited and specified Business Purposes described in Attachment 1 of this Addendum.

2.2 Client represents and warrants that it has complied with Privacy Laws in all material respects in relation to all Personal Information Processed by VL on Client's behalf pursuant to this Addendum.

## 3 Obligations of VL

3.1 VL shall process Personal Information disclosed to VL by Client only on behalf of and in accordance with the Instructions of Client, unless VL is otherwise required by Privacy

Laws, in which case, VL shall inform Client of such legal requirement before Processing Personal Information, unless informing the Client is prohibited by law. VL shall inform Client if, in VL's reasonable opinion, an Instruction infringes Privacy Laws. Client acknowledges that VL is under no obligation to perform a detailed legal examination with respect to the compliance of Client's Instructions with Privacy Laws. In the event that VL determines that an Instruction infringes Privacy Laws, VL shall not be liable to Client under the Agreement for failure to perform applicable Services until such time as Client issues new and lawful instructions with regard to the Processing of Personal Information.

3.2 VL shall maintain Personal Information in strict confidence and shall ensure that any VL personnel authorized to access and Process Personal Information are subject to confidentiality obligations with respect to the Personal Information.

3.3 VL shall not Sell or Share Personal Information. Except as described in Section 3.6 below, VL shall not (1) retain, use, or disclose Personal Information (i) for any purpose other than for the Business Purposes specified in Attachment 1 of this Addendum, or (ii) outside of the direct business relationship between Client and VL, or (2) combine Personal Information received pursuant to the Agreement with personal information received from or on behalf of another person(s), or collected from VL's own interaction with individuals, unless permitted by Privacy Laws.

3.4 For the avoidance of doubt, VL may, as part of providing the Services, Deidentify or Aggregate Personal Information in accordance with the standards for such activity set forth in applicable Privacy Laws.

3.5 VL shall comply with applicable obligations under Privacy Laws and provide the level of privacy protection for Personal Information as is required by applicable Privacy Laws. VL shall notify Client if VL makes a determination that it can no longer meet its obligations under this Addendum or applicable Privacy Laws.

3.6 To the extent permitted by Privacy Laws, VL may retain, use, or disclose Personal Information obtained in the course of providing the Services: (1) to retain and employ another Service Provider or Contractor as a Sub-Processor, where the Sub-Processor meets the requirements for a Service Provider or Contractor under the CCPA; (2) for internal use by VL to build or improve the quality of the services it provides to Client, provided that VL does not use the Personal Information to perform services on behalf of another person; (3) to prevent, detect, or investigate data security incidents, or protect against malicious, deceptive, fraudulent, or illegal activity; (4) to comply with federal, state, or local laws or comply with a court order or subpoena to provide information; (5) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; (6) to cooperate with law enforcement agencies concerning conduct or activity that VL reasonably and in good faith believes may violate federal, state, or local law; (7) to cooperate with a government agency request for emergency access to a consumer's Personal Information if a natural person is at risk or danger of death or serious physical injury, provided that (a) the request is approved by a high-ranking agency officer for emergency access to a consumer's Personal

Information, (b) the request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis, or (c) the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted; (8) to exercise or defend legal claims; (9) to collect, use, retain, Sell, Share, or disclose consumers' Personal Information that is Deidentified or Aggregate consumer information; or (10) collect, Sell, or Share a consumer's Personal Information if every aspect of that commercial conduct takes place wholly outside of California.

## 4 Data Transfers

4.1 VL and Client agree to comply with (i) the EU Standard Contractual Clauses, attached at Exhibit 1; and (ii) the UK Addendum to the EU Standard Contractual Clauses, attached at Exhibit 2, each to the extent applicable and required by Privacy Laws.

4.1.1 In the event Personal Information subject to the GDPR is transferred to a country outside the EEA, the EU Standard Contractual Clauses attached at Exhibit 1 shall apply.

4.1.2 In the event Personal Information subject to the UK GDPR is transferred to a country outside the UK, the UK Addendum to the EU Standard Contractual Clauses attached at Exhibit 2 also shall apply.

4.2 If Client is located in Switzerland and is subject to the Swiss DPA, then the EU Standard Contractual Clauses attached at Exhibit 1 shall be amended as follows with respect to Personal Information transferred to VL that is subject to the Swiss DPA:

4.2.1 References to a "data subject" shall include a legal person;

4.2.2 References to the GDPR shall be interpreted as references to the Swiss DPA, and references to an "EU Member State" shall include Switzerland.

4.2.3 To the extent Client is subject to both the GDPR and the Swiss DPA, the competent supervisory authority for purposes of Clause 13 of the EU Standard Contractual Clauses, shall be (i) the supervisory authority as set forth in Annex I.C for purposes of the GDPR, and (ii) the Swiss Federal Data Protection and Information Commissioner for purposes of the Swiss DPA;

4.2.4 To the extent Client is subject to the Swiss DPA and is not subject to the GDPR, the competent supervisory authority for purposes of Clause 13 of the EU Standard Contractual Clauses shall be the Swiss Federal Data Protection and Information Commissioner;

4.2.5 For the purposes of Clause 18(c) of the EU Standard Contractual Clauses, data subjects who are habitually resident in Switzerland may bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland;

4.3 VL shall not transfer Personal Information originating from inside the EEA, Switzerland, or the UK outside the EEA, Switzerland, or the UK for Processing unless it has executed the Processor-to-Processor EU Standard Contractual Clauses and, if applicable, the UK Addendum to the EU Standard Contractual Clauses, with the recipient of the Personal Information, or another appropriate data transfer mechanism applies.

## 5 Sub-Processing

5.1 Client consents to VL engaging Sub-Processors for the Processing of Personal Information in accordance with this Addendum. Where VL engages a Sub-Processor to assist with Processing Personal Information, VL shall enter into a written agreement with the Sub-Processor that imposes obligations on the Sub-Processor that are equivalent to those imposed on VL under this Addendum. VL may engage the Sub-Processors to assist with Processing Personal Information. If VL engages a new Sub-Processor to assist with Processing Personal Information, or changes Sub-Processors, VL will provide Client with at least 14 business days' notice of the appointment or change. If Client does not object to the appointment or change of the Sub-Processor on reasonable grounds within 10 business days of notification, the appointment or change will be deemed authorized. VL shall remain liable to Client for its obligations under this Addendum.

## 6 Information Security

6.1 VL shall develop, implement, and maintain appropriate administrative, technical, and organizational safeguards and other security measures ("Information Security Measures") to protect Personal Information received from Client.

6.2 Upon the expiration or earlier termination of the Agreement, or such earlier time as Client requests, VL shall ensure the prompt and secure disposal, or return to Client, of all copies of Personal Information received from Client in VL's custody or control, unless VL is required to retain Personal Information under Privacy Laws or other applicable law or regulatory requirements, or where retention is part of VL's ordinary records retention and backup practices, provided that VL will continue to treat the Personal Information in accordance with this Addendum. VL shall ensure compliance with Client's reasonable Instructions with respect to the return or disposal of Personal Information.

## 7 Information Security Incident Notification

7.1 VL shall promptly and without undue delay inform Client of any Information Security Incident of which VL becomes aware and shall reasonably cooperate with Client in all reasonable and lawful efforts to prevent, mitigate, or rectify such Information Security Incident. VL shall provide such assistance as reasonably required to enable Client to satisfy Client's obligations under Privacy Laws.

## 8 Monitoring and Other Assistance

8.1 VL shall, at the reasonable request of Client, make available to Client all information in its possession reasonably necessary to demonstrate compliance with the obligations set forth in this Addendum and applicable Privacy Laws. Once a year, and at no cost to VL,

VL shall allow for and cooperate with reasonable assessments, including audits and inspections, conducted by Client (or Client's designee, provided such designee is acceptable to VL and bound by confidentiality obligations satisfactory to VL), or alternatively arrange for such assessment by a qualified independent assessor of Client's choosing, of VL's policies and technical and organizational measures in support of applicable obligations under Privacy Laws. Client shall provide VL at least 30 days' prior written notice of its intention to carry out any such assessment, and such assessment shall be carried out during working hours on business days.

8.2 Client may take reasonable and appropriate steps to ensure that VL uses Personal Information in a manner consistent with Client's obligations under applicable Privacy Laws. Client may, upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

8.3 VL shall promptly inform Client of any formal requests from Data Subjects exercising their rights under Privacy Laws, and not respond to such requests unless instructed by Client in writing to do so. Client shall inform VL of any requests from Data Subjects with which VL must comply and provide the information necessary for VL to comply with the request. Taking into account the nature of the Processing of Personal Information, VL shall reasonably assist Client in fulfilling Client's obligations to respond to a Data Subject's request.

8.4 VL shall reasonably assist Client in complying with its obligations under Privacy Laws, in particular Client's obligation to implement appropriate Information Security Measures, to carry out a data protection impact assessment, and to consult a competent supervisory authority, as applicable.

## 9 Remedies

9.1 The Parties agree that: (i) that the Client entity that is the contracting party to the Agreement shall solely exercise any right or seek any remedy of authorized Affiliates under this Addendum on behalf of its Affiliates, and (ii) Client that is the contracting party to the Agreement shall exercise any rights under this Addendum in a combined manner for itself and on behalf of all of its Affiliates together. The Client entity that is the contracting entity is and shall be responsible for coordinating all instructions, authorizations, and communications pursuant to this Addendum and shall be entitled to make and receive all communications related to this Addendum on behalf of Affiliates.

## 10 General Provisions

10.1 If any provision of this Addendum is found by the applicable supervisory authority to be invalid or unenforceable, the validity and enforceability of the other provisions shall not be affected. This Addendum shall be governed by and construed in accordance with the laws of the Agreement between the parties, unless otherwise required by applicable Privacy Laws. By signing the Agreement, Client enters into this Addendum on behalf of itself and any Affiliates. The legal entity agreeing to this Addendum as Client represents

and warrants that it is authorized to agree to and enter into this Addendum for and on behalf of itself, and as applicable, each Affiliate.

Each person executing this Agreement represents and warrants that they have been authorized to do so and have the authority to bind the respective entity on whose behalf they are signing. The Parties hereby acknowledge that this Agreement may be executed and delivered by email and such document shall constitute a legal and binding agreement on the Parties and shall be considered effective as of the last date of execution below ("Execution Date").

## EXHIBIT 1

## EU STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

This Exhibit 1 is part of and subject to the terms of the Addendum and Agreement.

For the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization: **The data exporter is the entity identified as "Client" in the Addendum and Agreement to which this Exhibit is attached.**

Address: **As provided in the Agreement to which this Exhibit is attached.**

(the data **exporter**)

And

Name of the data importing organization: **Visual Lease, LLC**

Address: **100 Woodbridge Center Drive, Suite 200, Woodbridge, New Jersey 07095, USA**

(the data **importer**)

each a 'party'; 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 personal data.

### 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.

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

*Clause 3*

***Third-party beneficiaries***

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

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

*Clause 4*

***Interpretation***

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

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

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

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

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

*Clause 7*

***Docking clause***

(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.

**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 noncompliance. 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 subprocessors at least 14 business 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.[1] 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 subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential

[1] This requirement may be satisfied by the sub-processor acceding to these Clauses in accordance with Clause 7.

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 subprocessor to fulfil its obligations under that contract.

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

*Clause 10*

***Data subject rights***

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

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

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

*Clause 11*

***Redress***

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

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

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

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

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

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

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

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

*Clause 12*

***Liability***

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

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

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

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

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

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

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

*Clause 13*

***Supervision***

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1), the supervisory authority of the Member State in which the representative within the Article 27(1) is established, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2), the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, 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[2];

(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

[2] 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.

application of such laws in practice that is not in line with the requirements in paragraph (a).

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

*Clause 15*

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

**15.1 Notification**

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

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

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

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the

contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

**15.2 Review of legality and data minimisation**

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

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

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

## SECTION IV – FINAL PROVISIONS

*Clause 16*

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

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

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

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

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

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

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

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

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

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

*Clause 17*

***Governing law***

These Clauses shall be governed by the law of 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 the EU Member State where 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 the 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

## ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):**

Name: **The data exporter is the entity identified as "Client" in the Addendum and Agreement to which this Appendix is attached.**

Address: **As provided in the Agreement to which this Appendix is attached.**

Contact person's name, position and contact details: **As provided in the Agreement to which this Appendix is attached.**

Activities relevant to the data transferred under these Clauses: **Receipt of the Services under and in accordance with the Addendum and Agreement to which these Clauses are incorporated.**

Signature and date: **The Parties agree that execution of the Agreement shall constitute execution of the EU Standard Contractual Clauses.**

Role: Controller

**Data importer(s):**

Name: **Visual Lease, LLC**

Address: **100 Woodbridge Center Drive, Suite 200, Woodbridge, New Jersey 07095, USA**

Contact person's name, position and contact details: **Adam Francoeur, Vice President, Legal legal@visuallease.com**

Activities relevant to the data transferred under these Clauses: **Provision of the Services under and in accordance with the Addendum and Agreement to which these Clauses are incorporated.**

Signature and date: **The Parties agree that execution of the Agreement shall constitute execution of the EU Standard Contractual Clauses.**

Role: Processor

### B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred:***

- Employees and other personnel of the data exporter.
- Entities receiving services from the data exporter.

***Categories of personal data transferred:***

Identity/identification data (e.g., name, user ID); Contact information (e.g., email or postal address, telephone number); Professional details (e.g., title, company, role); Financial details (e.g., transaction data, financial account details); Online activity/device data (e.g., device ID, login ID, timestamp data, IP address, logs); and all other information required for the Services under the Agreement.

***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.***

None.

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

Client personal data may be transferred on a continuous basis, as determined by Client's use of the Services under the Agreement.

***Nature of the processing:***

Processing as necessary for the data importer to provide the Services under the Agreement, including (without limitation) accessing, storing, transmitting, analyzing, managing, and manipulating the personal data.

***Purpose(s) of the data transfer and further processing:***

Transfer and processing as necessary for the provision and receipt of the Services under and in accordance with the Agreement.

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

For the duration of the Agreement until deletion in accordance with the relevant provisions of the Addendum.

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

| **Infrastructure & Sales Enablement Sub-Processors** |
| --- |
| *VL may use the following Sub-Processors to provide infrastructure that assists with the delivery of VL Services:* |

| Sub-Processor | Location of Sub-Processor | Subject Matter of Processing | Nature of Processing |
|---|---|---|---|
| Pendo.io | 301 Hillsborough Street, Raleigh, NC 27603, USA | Product Analytics | **Combining powerful software usage analytics with in-app guidance and user feedback capabilities on behalf of VL** |
| Jira | 350 Bush Street, Floor 13, San Francisco, CA 94104, USA | Customer Support and Account Management | **Bug/issue tracking in-app tool on behalf of VL** |
| Salesforce | 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, USA | Customer Support and Account Management | **Manage customer data, sales operations, and marketing campaigns on behalf of VL** |
| Amazon Web Services | 410 Terry Avenue N., Seattle, WA, 98109, USA | Cloud Infrastructure | **Providing compute power, content delivery, database storage, etc., on behalf of VL** |
| Hubspot | 25 1st Street, Cambridge, MA 02141, USA | Customer Support and Account Management | **Providing a centralized customer database on behalf of VL** |
| OwnBackup | 940 Sylvan Avenue, Englewood Cliffs, NJ, 07632, USA | Backup Platform for Salesforce | **Provides cloud data protection on behalf of VL** |
| Salesloft | 1180 W. Peachtree Street, NW, Suite 600, Atlanta, GA 30305, USA | Customer Support and Account Management | **A cloud-based sales engagement platform on behalf of VL** |
| PowerBi (Microsoft) | One Microsoft Way, Redmond WA, 98052, USA | Product Analytics | **A data visualization and reporting platform on behalf of VL** |
| Drift | 222 Berkeley Street, Boston, MA 02116, USA | Customer Support Chatbox | **Facilitates communication with website visitors in real-time on behalf of VL** |
| Sendoso | 655 Montgomery Street, Suite 1720, San Francisco, CA 94111, USA | Account Management | **A platform for the delivery of corporate gifts on behalf of VL** |

| | | | |
|---|---|---|---|
| Vonage Contact Center | 23 Main Street, Holmdel, NJ 07733, USA | Customer Support | **Providing integrated communication services on behalf of VL** |
| Seismic | 12390 El Camino Real, San Diego, CA 92130, USA | Sales Support | **Sales enablement and digital sales engagement solution on behalf of VL** |
| Clari | 1154 Sonora Court, Sunnyvale, CA, 94086, USA | Sales and Account Management | **Manage sales pipeline and forecast future revenue on behalf of VL** |
| Zoom | 55 Almaden Blvd., 6th Fl, San Jose, CA, 95113, USA | Video Conferencing System | **Software-based video conferencing solutions** |

## C. COMPETENT SUPERVISORY AUTHORITY

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

**Clause 13 shall apply as follows: Where Client is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Client with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.**

**Where Client is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with 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 shall act as competent supervisory authority.**

**Where Client is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the Data Protection Commission of Ireland shall act as competent supervisory authority.**

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

*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.*

VL shall maintain compliance with the security principles as outlined in the GDPR and UK GDPR.

***Measures of pseudonymisation and encryption of personal data:***

- Encryption at rest and encryption in transit;
- Encryption key kept in the US;

***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:***

- Confidentiality arrangements;
- Information security policies and procedures;
- Backup procedures;
- Remote storage;
- Mirroring of hard disks (e.g., RAID technology);
- Uninterruptible power supply;
- Anti-virus/firewall protection, security patch management;
- Intrusion prevention, monitoring and detection;
- Availability controls to protect personal data against accidental destruction or loss;

***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:***

- Business continuity plan;
- Disaster recovery procedure;
- Incident response plan;

***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:***

- Internal and external audit program, audit reports and documentation;
- Periodic testing of back up processes and business continuity procedures;
- Risk evaluation and system monitoring on a regular basis;
- Vulnerability and penetration testing on a regular basis, not no less than annually;

***Measures for user identification and authorization:***

- Internal policies and procedures;
- User authentication controls, including secure methods of assigning selecting and storing access credentials and blocking access after a reasonable number of failed authentication access;
- Restricting access to certain users;
- Access granted based on a need-to-know, supported by protocols for access authorization, establishment, modification and termination of access rights;
- Logging and reporting systems;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;

***Measures for the protection of data during transmission:***

- Encryption in transit;
- Transport security;
- Network segregation;
- Logging;

***Measures for the protection of data during storage:***

- Encryption at rest;
- Access controls;
- Separation of databases and logical segmentation of VLC personal data from data of other vendor customers;
- Segregation of functions (production/testing/development);
- Procedures for storage, amendment, deletion, transmission of data for different purposes;

***Measures for ensuring physical security of locations at which personal data are processed:***

- Establishing security areas, restriction of access paths;

- Establishing access authorizations for employees and third parties with a need-to-know;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized processing equipment and personal computers;

***Measures for ensuring events logging:***

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Encryption at rest and in transit;

***Measures for ensuring system configuration, including default configuration:***

- Up-to-date baseline configuration documentation and settings;

***Measures for internal IT and IT security governance and management:***

- Information security policies and procedures;
- Incident response plan;
- Regular internal and external audit;
- Review and supervision of information security program;

***Measures for certification/assurance of processes and products:***

- SOC I, Type 2

***Measures for ensuring data minimisation:***

- Documentation regarding which data categories need to be processed;
- Ensure that the minimum amount of data is processed to fulfill the purpose of the processing;

***Measures for ensuring data quality:***

- Personal data is kept accurate and up to date;
- Data is corrected upon request or where necessary;

***Measures for ensuring limited data retention:***

- Records retention schedule;
- Data retention policy;
- Personal data is deleted or irreversibly anonymized after expiration of the retention period or deleted post-termination upon written request from Client Administrator;

***Measures for ensuring accountability:***

- Internal policies and procedures;
- Records of data processing activities;
- Adequate agreements with third parties;
- Vendor onboarding process and questionnaire;
- Monitoring of contract performance;
- InfoSec training program;

***Measures for allowing data portability and ensuring erasure:***

- Personal data is made available upon request in an electronically portable format using industry standards;
- Reduction methods are used, where necessary;
- Secure disposal of information stored on magnetic and non-magnetic media that prevents potential recovery of the information.

*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*

Data importer maintains a process to ensure that each sub-processor that processes personal data of data exporter is required to:

i. Process personal data only on behalf of and in accordance with the instructions of the data importer;

ii. Inform the data importer of any requests from data subjects to exercise their rights under the GDPR, and to provide assistance to the data importer in relation to the handling of such requests;

iii. Assist the data importer in relation to its obligations to (a) implement appropriate technical and organizational measures to ensure the security of data processing, (b) carry out a data protection impact assessment, and (c) to the extent required by applicable law, consult with the relevant supervisory authority, and assist the data importer in relation to the data importer's obligations to provide the same assistance to the data exporter;

iv. Implement, maintain and comply with a documented procedure for reviewing and responding to requests to access or disclose personal data that are received from foreign government authorities;

v. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with the processing by the sub-processor;

vi. Delete personal data or return it to the data importer on termination of the relationship between the data importer and sub-processor; and

vii. Notify the data importer of a personal data breach and provide reasonable assistance to the data importer to prevent, mitigate, or rectify such personal data breach, and to enable the data importer to satisfy its obligation to notify the data exporter of a personal data breach.

## EXHIBIT 2

## UK ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

### PART 1: TABLES

**Table 1: Parties**

| | | |
|---|---|---|
| **Start date** | The date of the Agreement | |
| **The Parties** | **Exporter**<br>**(who sends the Restricted Transfer)** | **Importer**<br>**(who receives the Restricted Transfer)** |
| **Parties' details** | Full legal name: **The exporter is the entity identified as "Client" in the Addendum and Agreement to which this Exhibit is attached.**<br>Trading name (if different):<br>Main address (if a company registered address): **As provided in the Agreement to which this Exhibit is attached.**<br>Official registration number (if any) (company number or similar identifier): | Full legal name: **Visual Lease, LLC**<br>Trading name (if different):<br>Main address (if a company registered address): **100 Woodbridge Center Drive, Suite 200, Woodbridge, New Jersey 07095, USA**<br>Official registration number (if any) (company number or similar identifier): |
| **Key contact** | Full name (optional):<br>Job title:<br>Contact details including email: **As provided in the Agreement to which this Exhibit is attached.** | Full name (optional): **Adam Francoeur**<br>Job title: **Vice President, Legal**<br>Contact details including email: **legal@visuallease.com** |
| **Signature**<br>**(if required for the purposes of Section 2)** | **The Parties agree that execution of the Agreement shall constitute execution of this UK Addendum to EU Standard Contractual Clauses.** | **The Parties agree that execution of the Agreement shall constitute execution of this UK Addendum to EU Standard Contractual Clauses.** |

**Table 2: Selected SCCs, Modules, and Selected Clauses**

| | |
|---|---|
| **Addendum EU SCCs** | ☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: **The date of the Agreement**<br>Reference (if any):<br>Other identifier (if any):<br>Or<br>☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses, or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |

| Module | Module in operation | Clause 7 (Docking Clause) | Clause 11 (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
|---|---|---|---|---|---|---|
| 1 | N/A | N/A | N/A | | | |
| 2 | N/A | N/A | N/A | N/A | N/A | |
| 3 | N/A | N/A | N/A | N/A | N/A | |
| 4 | N/A | N/A | N/A | | | N/A |

**Table 3: Appendix Information**

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

| |
|---|
| Annex I.A: List of Parties: Table 1 above |

| |
|---|
| Annex I.B: Description of Transfer: Annex I.B of the EU Standard Contractual Clauses attached at Exhibit 1 to this Addendum |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II of the EU Standard Contractual Clauses attached at Exhibit 1 to this Addendum |
| Annex III: List of Sub-Processors (Modules 2 and 3 only): Annex I.B of the EU Standard Contractual Clauses attached at Exhibit 1 to this Addendum |

**Table 4: Ending this Addendum when the Approved Addendum Changes**

| | |
|---|---|
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section 19:<br>☒ Importer<br>☐ Exporter<br>☐ neither Party |

**PART 2: MANDATORY CLAUSES**

**Entering into this Addendum**

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex I.A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

| | |
|---|---|
| Addendum | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| Addendum EU SCCs | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| Appendix Information | As set out in Table 3. |
| Appropriate Safeguards | The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved Addendum | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18. |
| Approved EU SCCs | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| ICO | The Information Commissioner. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR. |
| UK | The United Kingdom of Great Britain and Northern Ireland. |
| UK Data Protection Laws | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | As defined in section 3 of the Data Protection Act 2018. |

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such

amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

**Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

**Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is

resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

FOR A SIGNED COPY OF THIS AGREEMENT PLEASE EMAIL: legal@visuallease.com