VISUAL LEASE

Visual Lease Data Processing Agreement

BY ACCEPTING THIS DATA PROCESSING ADDENDUM OR ACCESSING OR USING THE SERVICES, YOU ARE AGREEING TO THE TERMS AND CONDITIONS OF THIS DATA PROCESSING AGREEMENT.

The Parties entered into an Agreement which requires the Processor to Process Personal Data. This agreement to Process such Personal Data, together with its exhibits ("Data Processing Addendum") specifies the obligations of the Parties when VLC is acting as a Processor.

This Data Processing Addendum is entered into by and between VLC, Inc., a Delaware-based Limited Liability Corporation ("VLC", "VL" or "Processor") and the person or entity that places the order for access to the VLC Platform or accesses the VLC Platform pursuant to a valid VLC Order Form ("Client" or "Controller"). Processor and Controller are individually referred to as "Party" and collectively as "Parties". The "Effective Date" of this Data Processing Addendum shall be the date which is the earlier of: a) Client's initial access to the VLC Platform; or b) the effective date of the first Order Form, as applicable. In consideration of the terms and conditions set forth below, the Parties agree as follows:

1. ***Definitions***

"CCPA" means the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020), California Civil Code Section 1798.100 et seq., and its implementing regulations.

"Controller" means the natural or legal person, corporate entity or non-profit organization, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Protection Laws" means applicable international, federal, state, and local legislation, rules, regulations and governmental requirements relating to the privacy or security of Personal Data, including without limitation and where applicable, European Data Protection Laws and the CCPA, in each case as amended, repealed, consolidated or replaced from time to time.

"Data Subject" means the individual to whom the Personal Data relates.

“Europe” means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom (“UK”).

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

“European Data Protection Laws” means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council 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 (“GDPR”); (ii) Direction 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) GDPR as it may be applies to the domestic laws of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act of 2018 (“UK GDPR”); and (iv) the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance(s) (“Swiss Data Processing Agreement”); in each case, as may be amended, superseded, or replaced from time to time.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data.

“Permitted Affiliates” means any of your Affiliates (as defined in the Terms) that: (i) are permitted to use the Subscription Services pursuant to the Agreement between the parties, but have not signed its own Agreement with VLC and are not a “Client” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by VLC, and (iii) are subject to Data Protection Laws.

“Personal Data” means any information (i) relating to an identified or identifiable individual, or (ii) that is otherwise protected as ‘personal data’, ‘personal information’, or ‘personally identifiable information’ under Data Protection Laws, where such information is contained within End User Data and is Processed by VLC in connection with the Agreement.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data transmitted, stored or otherwise Processed by VLC and/or our Subprocessors in connection with the provision of Subscription Services which would require notification under Data Protection Laws.

“Privacy Shield” means the EU-US and Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce and approved by the European Commission pursuant to its Decision of 12 July, 2016 and by the Swiss Federal Council on 11 January, 2017, respectively, and as may be amended, superseded, replaced, or updated from time to time.

“Privacy Shield Principles” means the Privacy Shield Principles (as supplemented) contained in Annex II to the European Commission Decision of 12 July, 2016 and as may be amended, superseded, replaced, or updated from time to time.

"Processing" means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "Process", "Processes" and "Processed" shall be construed accordingly.

"Processor" means a natural or legal person, public authority, agency, or other organized body which Processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the standard contractual clauses for Processors (Module Two) annexed to the European Commission Decision (EU) 2021/914 of 4 June, 2021, in the form set out at Attachment 1, as may be amended, superseded, or replaced.

"Subprocessor" means any Processor engaged by VLC or its Affiliates to assist in fulfilling its obligations with respect to the Platform and Services under the Agreement. Subprocessors may include entities unaffiliated with VLC, as well as VLC Affiliates.

"UK Addendum" means the UK Addendum to the Standard Contractual Clauses, in the form set out in Attachment 2.

2. *Processor Obligations*

2.1 Processor shall comply with this Data Processing Addendum at all times during the term of the Agreement. The rights and obligations of the Parties with respect to Processing Activities are described herein and in the Agreement between the Parties. The subject matter, nature, purpose, and duration of Processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this Data Processing Addendum. Processor shall Process Personal Data solely for the purpose of carrying out the Services, as specified in Exhibit A, and in accordance with Controller's Instructions, unless Processor is otherwise required by Data Protection Laws. Processor shall inform Controller if, in Processor's reasonable opinion, an Instruction infringes Data Protection Laws. Controller acknowledges that Processor is under no obligation to perform a detailed legal examination with respect to the compliance of Controller's Instructions with Data Protection Laws. In the event that Processor determines that an Instruction infringes Data Protection Laws, Processor shall not be liable to Controller under the Agreement for failure to perform applicable Services until such time as Controller issues new and lawful instructions with regard to the Processing of Personal Data.

2.2. Processor shall comply with Data Protection Laws directly applicable to Processor in connection with the Processing of Personal Data by Processor.

2.3 Processor shall maintain Personal Data in strict confidence and shall ensure that persons authorized to access Personal Data are subject to confidentiality obligations. Processor shall implement technical and organizational security measures designed to ensure a level of security appropriate to the risk and prevent Personal Data Breaches.

2.4 Upon receipt of Controller's written request following the termination or expiration of VLC's provision of the Platform or Services for any reason, Processor shall ensure the prompt and secure disposal or, a return to Controller of all copies of Personal Data (except where retention of the Personal Data is required by applicable law or regulatory requirements, or where retention is part of Processor's ordinary records retention and backup practices, provided that Processor will continue to treat the Personal Data in accordance with this Data Processing Addendum). Processor shall ensure compliance with Controller's reasonable instructions with respect to the return or disposal of Personal Data.

3. *Client Obligations*

3.1 Controller Instructions. The Parties agree that the Agreement, including this Data Processing Addendum, constitutes your Instructions to Processor in relation to the Processing of Personal Data, and that these Instructions constitute the complete Instructions during the Initial Term and any subsequent Term. Upon the mutual written agreement of the Parties, Controller may provide additional instructions during the Initial Term or any subsequent Term that are consistent with the Agreement, including this Data Processing Addendum.

3.2 Compliance with Laws. Client shall be responsible for complying with all Data Protection Laws applicable to its use of the Platform and Services, its Processing of Personal Data, and its Instructions to Processor, including providing any necessary notices and obtaining any necessary consents and authorizations.

3.3 Controller shall be solely response for: (i) the accuracy, quality, and legality of End User Data and the means by which Controller acquired Personal Data that is disclosed or otherwise made available to Processor; (ii) ensuring Controller has the right to disclose or otherwise make available Personal Data to Processor for Processing in accordance with the terms of the Agreement between the Parties (including this Data Processing Addendum); (iii) informing Processor without undue delay if Controller is not able to comply with Controller's obligations under Data Protection Laws.

4. *Personal Data Breaches*

Processor shall notify Controller without undue delay, but in no event less than seventy-two (72) hours after it becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Controller. At Controller's request, Processor shall provide Controller with such reasonable assistance as necessary to enable Controller to notify relevant affected data subjects and/or applicable data authorities in accordance with its obligations under Data Protection Laws.

5. *Data Subject Requests and other Assistance*

5.1 Processor shall assist Controller in connection with its obligations under Data Protection Laws, including Controller's obligations to carry out a data protection impact assessment, and to consult the competent regulators, and responding to requests from Data Subjects to exercise their rights under Data Protection Laws ("Data Subject Requests"). To the extent that Controller is

unable to independently address a Data Subject Request, then upon Controller's written request Processor shall provide reasonable assistance to Controller to respond to any Data Subject Requests relating to the Processing of Personal Data under the Agreement. Processor will attempt to provide such assistance as may be required to address such requests at no cost to Controller, but reserves the right to charge commercially reasonable costs arising from such assistance.

5.2 If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Processor, Processor shall promptly inform Controller and will advise the Data Subject to submit their request directly to the Controller. Controller shall be solely responsible for responding substantively to any Data Subject Requests or communications involving Personal Data.

6. *Subprocessors*

Controller agrees that Processor may engage Subprocessors (which may include affiliates of Processor) to process Personal Data solely in performance of the Services as provided in the Agreement and that Processor shall publish a list of current Subprocessors through an RSS feed made available to Controller. Processor shall (i) notify Controller prior to any changes to Processor's active Subprocessor list; and (ii) provide Controller the opportunity to object to such changes within ten (10) business days after receipt of Processor's notice on legitimate grounds relating to the relevant Subprocessor's ability to protect Personal Data in accordance with the terms of this Data Processing Addendum. When Processor engages Subprocessors, Processor shall impose data protection terms on Subprocessors providing for at least the same level of protection for Personal Data as those in this Data Processing Addendum to the extent applicable to the nature of the services provided by such Subprocessors. Processor shall remain responsible for each Subprocessor's compliance with the obligations of this Data Processing Addendum as well as for any acts or omissions of such Subprocessor that shall cause Processor to breach any of its obligations under this Data Processing Addendum.

7. *Data Transfers*

7.1 Where the Services involve the transfer of European Data to the Processor in a country which has not been deemed to provide an adequate level of data protection pursuant to European Data Protection Laws ("Adequacy Decision"), the following applies:

1. a) With respect to transfers outside the European Economic Area, the Parties shall comply with the terms of the Standard Contractual Clauses. If there is any conflict between the Standard Contractual Clauses and this Data Processing Addendum, the Standard Contractual Clauses shall apply.
2. b) With respect to transfers outside the UK, the Parties shall comply with the terms of the Standard Contractual Clauses as amended by the UK Addendum.

3. c) at Controllers request, the Standard Contractual Clauses shall be replaced and the Parties shall execute new standard contractual clauses for transfers to data processors in third countries adopted pursuant to Art. 46 (2) c) or d) of the GDPR.
4. d) If an Adequacy Decision is repealed or suspended, paragraphs a) and b) above shall automatically apply.

7.2 UK Transfers Pursuant to the UK Addendum. The Parties acknowledge that following entry into this Data Processing Addendum, the UK may adopt a new set of approved standard contractual clauses that the Parties will be required to execute ("New Approved UK Clauses") and incorporate into this Data Processing Addendum in place of the Standard Contractual Clauses as amended by the UK Addendum. In the event New Approved UK Clauses are adopted, the Parties shall work together in good faith and in a timely manner to ensure any formal deadline for implementation of the New Approved UK Clauses is met, including by taking such actions (which may include execution of documents or an addendum to this Data Processing Addendum) as may be required to give effect to the New Approved UK Clauses to ensure compliance with the UK GDPR.

8. *California Personal Data*

For the purposes of this "California Personal Data" section the Data Processing Addendum, "Business Purpose," "Sell" (and its derivatives), "Share" (and its derivatives), and "Service Provider" have the meaning ascribed to them in the CCPA.

When, pursuant to the Agreement, Client discloses Personal Data to VLC that is directly subject to the CCPA ("California Personal Data"), the Parties acknowledge and agree that Client is a "Business" and VLC is a "Service Provider" for the purposes of the CCPA. Business and Service Provider agree that Service Provider shall Process California Personal Data for the purpose of performing the Services under the Agreement between the parties (which the parties acknowledge and agree are for Client's "Business Purpose") or as otherwise may be permitted by the CCPA or applicable law. Except where permitted by applicable law or the Data Processing Addendum, Service Provider shall not (1) Sell California Personal Data, (2) retain, use or disclose California Personal Data (i) for any purpose other than for the Business Purposes specified in the Agreement. For the avoidance of doubt, this "California Personal Data" section of the Data Processing Addendum shall only apply to California Personal Data.

9. *Monitoring*

Processor shall make available to Controller all information reasonably necessary to demonstrate compliance with the obligations set forth in this Data Processing Addendum and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller (provided such auditor is acceptable to Processor and bound by confidentiality obligations satisfactory to Processor) by providing Controller access to reasonable documentation evidencing Processor's compliance with this Data Processing Addendum. Controller shall provide a copy of the audit report to Processor which shall be treated as

Processor confidential information. Audits shall be conducted no more than once per year, during the term of the Agreement, during regular business hours, and shall be subject to (i) a written request submitted to Processor at least thirty (30) days in advance of the proposed audit date; (ii) a detailed written audit plan reviewed and approved by Processor. The audits shall not be permitted to disrupt Processor's Processing activities or compromise the security and confidentiality of Personal Data pertaining to other Processor customers. Processor may charge Controller a reasonable fee for such audit.

10. *Remedies*

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 Data Processing Addendum on behalf of its Affiliates, and (ii) Client that is the contracting party to the Agreement shall exercise any rights under this Data Processing 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 Data Processing Addendum and shall be entitled to make and receive all communications related to this Data Processing Addendum on behalf of Affiliates.

11. *General Provisions*

If any provision of this Data Processing 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 Data Processing Addendum shall be governed by and construed in accordance with the laws of the Agreement between the parties, unless otherwise required by applicable data protection laws. By signing the Agreement, Controller enters into this Data Processing Addendum on behalf of itself and any Affiliates. Capitalized terms not defined in this Data Processing Addendum shall have the meaning set forth in the Agreement between the Parties. The legal entity agreeing to this Data Processing Addendum as Client represents and warrants that it is authorized to agree to and enter into this Data Processing Addendum for and on behalf of itself, and as applicable, each Affiliate.

ATTACHMENT 1

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 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 importer'), 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 the 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 1.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein form 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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – 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 — 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 completed 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 through 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 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 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 local law. This is without prejudice to Clause 14, in particular the requirements 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 psuedonymisation, 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 subject 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.

(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 reasonably intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) 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 fulfills its 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

project business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

(e) the data importer shall agree [to] 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

Security Measures

(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 unless it has been authorised to do so by the data exporter.

(b) the data importer shall assist the date exporter in fulfilling its obligations to respond to data subjects' requests from 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 involves 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 the 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) 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[4];

(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 the laws or practices not in line with the requirements under paragraph (a), including following a change in laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter has reason to believe that the data importer can no longer fulfill 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 the 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 designation, 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) 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 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 Member State where 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 Member State where 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.

ANNEX I

1. LIST OF PARTIES

By accessing the VLC Platform or using the VLC Services where personal data is transferred from data exporter to data importer from a Member State or the United Kingdom, the Parties also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated as of the date of the Data Processing Addendum.

Data exporter(s):

- Name: The Client Address: As provided on the Order Form
- Contact person's name, position and contact details: As provided on the Order Form
- Activities relevant to the data transferred under these Clauses: As provided on the Order Form
- Signature and date: Order Form effective date
- Role (controller/processor): controller

Data importer(s):

- Name: VLC, Inc. Address: 100 Woodbridge Center Drive, # 200, Woodbridge, NJ 07095
- Contact person's name, position and contact details: Adam Francoeur, Vice President, Legal
- Activities relevant to the data transferred under these Clauses: Collection of data for the provision of platform services as provided on Order Form.
- Signature and date: Order Form effective date
- Role (controller/processor): processor

1. DESCRIPTION OF TRANSFER

- Categories of data subjects whose personal data is transferred:
    - Employees and other personnel (e.g., contractor) of Exporter
- Categories of personal data transferred (mandatory fields)[5]:

Mandatory fields

- User ID
- First Name
- Last Name
- Allow Import
- Allow Import Financials
- Straight Line Rent and Lease Accounting Edit Rights
- User Group
- Email Address
- Status
- Can View Projects
- Password
- Confirm Password
- Internet Protocol Address

Optional fields

- Phone
- Cell Phone
- Fax Number

- 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 for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
    - None required.
- The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
    - Continuous.
- Nature of the processing
    - Electronic data collection (manual entry, api feed)
- Purpose(s) of the data transfer and further processing:
    - For the provision of the Platform and Services
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
    - Contract term. Retained-post termination in accordance with this Data Processing Addendum.
- For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing:
    - Not applicable

1. COMPETENT SUPERVISORY AUTHORITY

- Identify the competent supervisory authority/ies in accordance with Clause 13:
    - The competent supervisory authority in the EU Member State in which the data exporter is established.

ANNEX II

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

VLC 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;

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.

ANNEX III

LIST OF EU/UK SUB-PROCESSORS

Available at: https://stavisuallease.wpengine.com/gdprsubprocessors/

Name	Purpose	Address (Headquarters)
Pendo.io	Product Analytics	301 Hillsborough Street, Raleigh, NC 27603, USA
Jira	Customer Support and Account Management	350 Bush Street, Floor 13, San Francisco, CA 94104, USA
Salesforce	Customer Support and Account Management	415 Mission Street, 3rd Floor, San Francisco, CA, 94105, USA
Amazon Web Services	Cloud Infrastructure	410 Terry Avenue N., Seattle, WA, 98109, USA

Hubspot	Customer Support and Account Management	25 1st Street, Cambridge, MA 02141, USA
OwnBackup	Backup Platform for Salesforce	940 Sylvan Avenue, Englewood Cliffs, NJ, 07632, USA
Salesloft	Customer Support and Account Management	1180 W. Peachtree Street, NW, Suite 600, Atlanta, GA 30305, USA
Gong	Customer Support and Account Management	265 Cambridge Avenue, Suite 60717, Palo Alto, CA 94306, USA
PowerBi (Microsoft)	Product Analytics	One Microsoft Way, Redmond WA, 98052, USA
Drift	Customer Support Chatbox	222 Berkeley Street, Boston, MA 02116, USA
Sendoso	Account Management	655 Montgomery Street, Suite 1720, San Francisco, CA 94111, USA
Vonage Contact Center	Customer Support	23 Main Street, Holmdel, NJ 07733, USA
Seismic	Sales Support	12390 El Camino Real, San Diego, CA 92130, USA
Clari	Sales and Account Managment	1154 Sonora Court, Sunnyvale, CA, 94086, USA

ATTACHMENT 2

UK ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

Date of this Addendum

1. The Clauses are dated as of the same date of the Data Processing Addendum. This Addendum is effective from: The same date as the Clauses.

Background

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

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

4.

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
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	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.
5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
6. 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

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate: a. for 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 transfer; and b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.
9. The amendments required by Section 7 above, include (without limitation):
10. References to the "Clauses" means this Addendum as it incorporates the Clauses;
11. 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."
12. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
13. References to Regulation (EU) 2018/1725 are removed.
14. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
15. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
16. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
17. Clause 18 is replaced to state: "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."
18. The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

Executing this Addendum

12. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):
13. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A: "By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum) "By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum) (or words to the same effect) and executing the Clauses; or
14. By amending the Clauses in accordance with this Addendum, and executing those amended Clauses.

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

[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 ensure 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 are set out in the contract or other legal act between the controller and thee 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 2021/915.

[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.

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

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosures 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 of 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.

[5] Fields listed above do not include optional fields or free-write content that may be processed and/or stored in the VLC platform at data exporter's election.