DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends and is incorporated into the software license agreement (together with any amendments and attached or referencing service orders, statements of work, attachments, schedules, or exhibits, the "**Agreement**") between ZoomInfo Technologies LLC or one of its Affiliates ("**Supplier**") and Customer as identified in the Agreement and will be applicable when Supplier is Processing Customer Personal Data on the behalf of Customer where such Processing is regulated by Applicable Laws.

This DPA applies to all activities related to the Agreement in which Supplier or third parties commissioned by Supplier may Process Personal Data on behalf of Customer in the course of providing services to Customer. It contains, in conjunction with the Agreement, the documented instructions for the Processing of Customer Personal Data as well as the subject-matter, duration, nature, and purpose of the Processing, which shall govern the rights and obligations of the parties in connection with the Processing of Personal Data.

1. Definitions

1.1 For the purpose of this DPA (i) "**Personal Data**" means any information relating to an identified or identifiable natural person; (ii) "**Data Subject**" means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, address, title, or an online identifier. In the context of the Agreement, (iii)"**Customer Personal Data**" means business contact information (such as name, work email address, work phone number) relating to Customer's personnel provided by Customer to Supplier for purposes of accessing Supplier's software and/or database; (iv) "**Processing**", "**Process**", "**Processed**" means any operation or set of operations which is performed on Customer Personal Data, individually or in sets, 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; (v) "**Affiliate**" means a business entity that directly, or through one or more intermediaries, controls or is controlled by or is under common control with a party. One entity is deemed to control the other if it directly or indirectly (a) owns more than fifty percent (50%) of the equity of the other entity or (b) controls more than fifty percent (50%) of the voting rights of the other entity; (vi) "**Applicable Law(s)**" means all laws applicable to the Processing of Customer Personal Data, which may include EU Data Protection Laws, other laws of the European Union or any Member State thereof, the UK GDPR, and the laws of any other country or state to which the Customer or the Customer Personal Data is subject. For the avoidance of doubt, all terms herein (whether in capital letters or lowercase) not otherwise defined but used in this DPA, shall have the meaning given to them in the Agreement, or if undefined in both documents, shall have the meaning as per the European General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) (as amended from time to time, "**GDPR**").

2. Data Processing

2.1 The parties acknowledge and agree that with regard to the Processing of Customer Personal Data on behalf of Customer, Customer is the Controller and Supplier is a Processor.

2.2 Any Processing of Personal Data by Supplier under this DPA shall occur only:

2.2.1 on behalf of Customer (including when Processing is initiated by Customer's Authorized Users);

2.2.2 in accordance with the Agreement; and

2.2.3 for the purpose of fulfillment of Customer's written instructions.

2.3 This DPA and the Agreement are Customer's complete instructions at the time of signature of this DPA to Supplier for the Processing of Customer Personal Data. However, such instructions may be amended, supplemented, or replaced by Customer in written or otherwise documented form at any time. If any new instructions from Customer exceed the scope of this DPA, they shall be considered as Customer's request to amend the DPA.

2.4 Supplier will Process Customer Personal Data for the duration of the Agreement or as indicated in documented instructions from the Customer, unless otherwise agreed upon in writing or required by Applicable Law.

2.5 The categories of Data Subjects affected by the Processing of Customer Personal Data on the behalf of Customer within the scope of this DPA will include Customer personnel designated by Customer as Authorized Users of Supplier's Services.

2.6 The types of Customer Personal Data affected by the Processing within the scope of this DPA will include business contact information (which may include the following or a subset: name, work email address, title, work phone number) relating to Customer personnel provided by Customer to Supplier for the purpose of accessing Supplier's Services.

2.7 The Customer Personal Data transferred will be subject to the following basic processing activities: to create authorized user accounts in Supplier's system, to provision access, identify segregated system user accounts, monitor system functionality and security, and related purposes.

3. CPRA

3.1 To the extent that Supplier Processes any Customer Personal Data relating to individuals who are California residents, Supplier shall comply with the requirements of the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq. ("**CPRA**"), including any amendments and implementing regulations that become effective on or after the effective date of this DPA, and shall provide the same level of privacy protection as is required by the CPRA. Capitalized terms used but not defined in this Section 3 shall have the same meaning as in the CPRA. For the purposes of the CPRA, the parties agree that Supplier is a "**Service Provider**" in the performance of its obligations, and that Customer is a "**Business**," and that the transfer of Customer Personal Data to Supplier shall not be considered a "Sale" or "Sharing." To the extent required by the CPRA, Supplier shall (a) grant Customer the right to take reasonable and appropriate steps to help ensure that Supplier uses Customer Personal Data in a manner consistent with Customer's obligations under the CPRA; (b) notify Customer if Supplier determines that it can no longer meet its obligations under the CPRA; and (c) grant Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data. To the extent required by the CPRA, Customer shall inform Supplier of any consumer requests made pursuant to the CPRA that they must comply with, and shall provide all information necessary for Supplier to comply with such request.

3.2 Supplier shall Process Customer Personal Data only for the "**Business Purposes**" specified in the Agreement and this DPA, including but not limited to (a) Supplier's operational purposes; (b) providing the Services to Customer; (c) auditing; (d) helping to ensure security and integrity; (e) debugging; (f) short-term, transient use; (g) providing advertising and marketing services to the extent such services are contemplated by the parties' Agreement; and (h) undertaking internal research for technological development and demonstration. The parties agree that Customer discloses Customer Personal Data to Supplier only for these limited purposes.

3.3 As a Service Provider, Supplier shall not:

3.3.1 Sell or Share Customer Personal Data;

3.3.2 retain, use, or disclose Customer Personal Data for any purpose other than for the Business Purposes specified in the Agreement and this DPA, including retaining, using, or disclosing Customer Personal Data for a commercial purpose other than the Business Purposes specified in the Agreement and this DPA, or as otherwise permitted by the CPRA;

3.3.3 retain, use, or disclose Customer Personal Data outside of the direct business relationship between Supplier and Customer; or

3.3.4 combine Customer Personal Data that Supplier receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Supplier may combine personal information to perform any Business Purpose as defined in the regulations adopted pursuant to paragraph (10) of subdivision (a) of Cal. Civ. Code § 1798.185, except as provided for in paragraph (6) of subdivision (e) of Cal. Civ. Code § 1798.140 and in regulations adopted by the California Privacy Protection Agency.

4. Other U.S. Data Protection Laws

4.1 To the extent that Supplier Processes any Customer Personal Data relating to individuals who are "**Consumers**" as that term is defined in the Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et seq. ("**CPA**"), the Connecticut Data Privacy Act, Public Act No. 22-15 ("**CTDPA**"), the Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq. ("**UCPA**"), and the Virginia Consumer Data Protection Act, Va. Code Ann. §§59.1-575 et seq. ("**VCDPA**") (collectively, the "**Consumer Privacy Laws**" or "**CPL**"), respectively, and upon the respective effective dates of the CPL, Supplier shall comply with the CPL's requirements, including any amendments and implementing regulations that become effective on or after the effective date of this DPA.

5. Independent Data Controllers

5.1 With respect to Personal Data which Supplier may provide Customer access to in the course of providing the Services, each agrees to comply with all applicable laws as it relates to the collection, Processing, and use of such Personal Data as independent Controllers of such information.

6. Personnel

6.1 The parties shall:

6.1.1 ensure all employees involved in Processing or transferring of Customer Personal Data have (1) either committed themselves to confidentiality in writing or have statutory or fiduciary obligations and (2) are authorized and appropriately trained to Process Customer Personal Data;

6.1.2 ensure the access to Customer Personal Data is limited to the personnel necessary to execute the party's obligations under the Agreement; and

6.1.3 appoint a data protection officer, if required by the Applicable Law, and provide his / her contact details on written request to the other party.

7. Technical and Organizational Measures

7.1 Supplier shall implement and maintain appropriate technical and organizational measures to provide a level of security appropriate to the risk for the Processing of Customer Personal Data. Supplier shall regularly test, assess, and evaluate the effectiveness of such technical and organizational measures for ensuring the security of the Processing.

8. Sub-Processors and Data Transfers

8.1 If such entities are deemed sub-processors, Customer hereby consents to the usage of Supplier's respective Affiliates and third-party service providers as sub-processors identified in Annex III to Schedule 1. Should Supplier add to or replace such sub-processors, Supplier shall provide a method for Customer to receive notice and an opportunity to object, provided such objection is based on reasonable grounds relating to data protection. If Customer does not object within 30 days, then such added or replaced sub-processors shall be considered incorporated into Annex III to Schedule 1 as an amendment.

8.2 Supplier shall impose substantially similar data protection obligations on any sub-processors (including its Affiliates) as set out in this DPA (in particular providing sufficient guarantees to implement appropriate technical and organizational measures). Supplier shall be liable for the acts and omissions of its sub-processors to the same extent Supplier would be liable if performing the services of each sub- processor directly under the terms of this DPA.

8.3 For any transfer of Customer Personal Data from a country inside the European Economic Area, the United Kingdom, or Switzerland to a country outside the European Economic Area, the United Kingdom, or Switzerland, applicable requirements of GDPR must be fulfilled. Customer authorizes Supplier to store or Process Customer Personal Data in the United States or any other country in which Supplier or its sub-processors maintain facilities. Customer appoints Supplier to perform any such transfer of Customer Personal Data to any such country and to store and Process Customer Personal

Data in order to provide the Services or by documented instructions of Customer. The parties will conduct all such activity in compliance with the Agreement, this DPA, and Applicable Law.

8.4 If Customer transfers Customer Personal Data originating from the EEA to Supplier when the Supplier is located in countries outside the EEA that have not received a binding adequacy decision by the European Commission, such transfers shall be made in compliance with applicable data transfer legal requirements and only by documented instructions from Customer. The parties acknowledge and agree to abide by the obligations set out in the Standard Contractual Clauses (European Commission Decision 2021/914 of 4 June 2021), found in Schedule 1, for any transfers of Customer Personal Data from within the EEA to outside of the EEA. For the purpose of processing Customer Personal Data under this DPA and the incorporation of the Standard Contractual Clauses, Module 2 of the Standard Contractual Clauses shall be applicable.

8.5 If Customer transfers Customer Personal Data originating from the UK to Supplier when Supplier is located in countries outside the UK that have not received an adequacy regulation by the UK Secretary of State for the Department for Digital, Culture, Media and Sport, then the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "**UK Addendum**") attached as Schedule 2 to this DPA shall apply in addition to the Standard Contractual Clauses in Schedule 1. The parties acknowledge and agree to abide by the obligations set out in the UK Addendum.

8.6 In relation to transfers of Customer Personal Data protected by the Swiss Federal Act on Data Protection ("**FADP**"), the Standard Contractual Clauses in Schedule 1 shall apply with the following modifications: (i) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the FADP and the equivalent articles or sections therein; (ii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and "Swiss law"; (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "competent Swiss courts"; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland. The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland). Until the revised FADP enters into force on September 1, 2023, data pertaining to legal entities are also protected by the FADP. The parties acknowledge and agree that, upon the effective date of the revised FADP on September 1, 2023, data pertaining to legal entities will no longer be protected.

9. Requests from Data Subjects

9.1 Supplier shall, in accordance with Applicable Laws, promptly notify Customer if Supplier receives a request from a Data Subject to which the Customer Personal Data relates to exercise his/her rights connected to the Processing under the Agreement and this DPA. Supplier shall use appropriate technical and organizational measures to cooperate and assist Customer in responding to such requests.

10. Security Breach

10.1 Supplier shall:

10.1.1 Notify Customer without undue delay after discovery and confirmation of any actual incident of unauthorized or accidental disclosure of or access to any Customer Personal Data or other breach of this DPA by Supplier or any of its staff, sub-processors, or any other identified or unidentified third party (the "**Security Breach**");

10.1.2 Provide Customer with reasonable cooperation and legally required assistance in respect of any Security Breach and all relevant information in Supplier's possession concerning the Security Breach, including, but not limited to, the following: (i) the nature of the breach; (ii) the categories and quantities of Customer Personal Data involved;
(iii) the name and contact details for the relevant contact person;

10.1.3 Take any necessary and legally required corrective or mitigating actions, pursuant to Applicable Laws and regulations, to remedy or mitigate any Security Breach; and

10.1.4 Not make any announcement or publish or otherwise authorize any broadcast of any notice or information about a Security Breach without notifying Customer unless legally required to do so.

11. Cooperation

11.1 In case of reporting and notification obligations to competent data protection supervisory authorities and/or affected Data Subjects resulting from Security Breaches the parties shall, upon request, provide reasonable support and information to the other party to comply with the investigation of any Security Breach and to fulfill any legally required obligations.

11.2 The parties will cooperate to the extent reasonably necessary in connection with their obligations to conduct data protection impact assessments and engage in consultation with supervisory authorities. If a supervisory authority corresponds with one party regarding either party's Processing of Customer Personal Data under the Agreement or this DPA, the party receiving the correspondence will promptly notify the other party. The parties will cooperate to the extent reasonably necessary to fulfill their obligations to respond to the supervisory authority's request. The parties will each bear the respective costs they incur when fulfilling such obligations.

12. Return and Deletion of Personal Data.

12.1 Customer Personal Data (including any copy of it) shall not be kept longer than is required for the Processing purposes or providing Services under the Agreement, unless (i) a longer retention period is required for audit, legal, or regulatory purposes or (ii) Customer instructs Supplier in writing to (a) keep certain Customer Personal Data longer or (b) return certain Customer Personal Data earlier.

12.2 The return or destruction of any data storage medium provided by Customer to Supplier shall be conducted without undue delay (i) after Processing is complete or termination / expiration of the Agreement or (ii) earlier, by written request of Customer.

13. Audits

13.1 Upon request but only for cause or to the extent required by Article 28 of the GDPR or other Applicable Law, Supplier will make available to Customer all relevant information necessary, and allow for and contribute to audits, including inspections, conducted by Customer, or another auditor who is not a competitor and agreed to in advance by Supplier, to demonstrate compliance hereunder. Such audits or inspections shall be limited to Supplier's Processing of Customer Personal Data in its capacity as a Data Processor only, not any other aspect of Supplier's business or information systems. If Customer requires Supplier to submit to audits or inspections that are necessary to demonstrate compliance, Customer will provide Supplier with written notice at least sixty (60) days in advance of such audit or inspection. Such written notice will specify the things, people, places, or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered Supplier's Confidential Information and, notwithstanding anything to the contrary in the Agreement, will remain Confidential Information in perpetuity or the longest time allowable by applicable law after termination of the Agreement. Such materials and derivative work product produced in response to Customer's request will not be disclosed to anyone without the prior written permission of Supplier unless such disclosure is required by applicable law. If disclosure is required by applicable law, Customer will give Supplier prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable law or order of a court or governmental agency. Customer will make every effort to cooperate with Supplier to schedule audits or inspections at times that are convenient to Supplier during usual business hours and without disturbance to Supplier's operations and personnel. Customer shall be solely responsible for all costs incurred in relation to audits or inspections.

14. Miscellaneous.

14.1 Without prejudice to any other obligations under this DPA or the Agreement, the parties will secure Customer Personal Data (i) with at least reasonable care and skill; and (ii) in accordance with good industry practice and Applicable Laws and regulations.

14.2 The term of this DPA corresponds to the term of the Agreement and any subsequent agreements referencing it between the parties. Provisions which by their nature are intended to survive termination or expiration of this DPA, will continue and survive any termination or expiration of this DPA.

14.3 Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail with respect to data privacy and security matters.

14.4 The effective date of this DPA is the date when Customer signs the Agreement that incorporates this DPA. The DPA will continue in effect until the Agreement and any subsequent agreements referencing it between the parties have terminated or been expired.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(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 – Optional

[INTENTIONALLY OMITTED]

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

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

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

Clause 9
Use of sub-processors

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

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, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([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 laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the 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 Ireland.

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 Ireland.

(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.

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

[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 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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):
Name: The entity identified as “Customer” or “Licensee” in the Agreement

Address: The contact details associated with Customer's ZoomInfo account or as otherwise specified in the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer's ZoomInfo account or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: To receive access to the ZoomInfo platform and ongoing support and services from ZoomInfo.

Role (controller/processor): Controller

Data importer(s):
Name: ZoomInfo Technologies LLC

Address: 805 Broadway, Suite 800, Vancouver WA 98660 USA

Contact person’s name, position and contact details: James Henry, Associate General Counsel, legal@zoominfo.com

Activities relevant to the data transferred under these Clauses: Customer data processing to provide services specifically requested by customer.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer personnel designated by Customer as Authorized Users of Supplier's Services

Categories of personal data transferred

Business contact information (which may include the following or a subset: name, work email address, title, work phone number) relating to Customer personnel provided by Customer to Supplier for the purpose of accessing Supplier's Services.

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.

No sensitive data transferred. Safeguards outlined in DPA and Annex II.

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

Typically, one-off but continuous transfers are conceivable depending on the nature of the services requested by Customer.

Nature of the processing

To create authorized user accounts in Supplier's system, to provision access, identify segregated system user accounts, monitor system functionality and security, and related purposes.

Purpose(s) of the data transfer and further processing

To create authorized user accounts in Supplier's system, to provision access, identify segregated system user accounts, monitor system functionality and security, and related purposes.

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

Subject to Section 12 of the DPA, Supplier will retain Customer Personal Data for as long as required for the Processing purposes or providing Services under the Agreement, unless (i) a longer retention period is required for audit, legal, or regulatory purposes or (ii) Customer instructs Supplier in writing to (a) keep certain Customer Personal Data longer or (b) return certain Customer Personal Data earlier.

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

For the duration of the Agreement or as indicated in documented instructions from the Customer, unless otherwise agreed upon in writing or required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

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

If Customer is established in an EU Member State, then the supervisory authority of that Member State.

If Customer is not established in an EU Member State, falls within the territorial scope of application of the regulation, and has appointed a representative, then the supervisory authority of the Member State that the representative is established.

If Customer is not established in an EU Member State, falls within the territorial scope of application of the regulation, and has not appointed a representative, then the Irish Data Protection Commission.

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.

The full text of ZoomInfo's technical and organizational security measures is available at https://www.zoominfo.com/about-zoominfo/security-overview ("**Security Overview**"). The full text of ZoomInfo's privacy policy is available at https://www.zoominfo.com/about-zoominfo/privacy-policy ("**Privacy Policy**").

Security Measure(s)	Evidence of Security Measure(s)
Measures of pseudonymisation and encryption of personal data	See Section 7.1 (Data Protection and Encryption) of the Security Overview
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See Sections 3 (Security Fundamentals), 7 (Prevention), and 8 (Detection) of the Security Overview
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	See Section 9 (Response) of the Security Overview
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	See Sections 7 (Prevention), 8 (Detection), and 9 (Remediation) of the Security Overview
Measures for user identification and authorisation	See Section 7.5 (Identity and Access Control) of the Security Overview
Measures for the protection of data during transmission	See Section 7.1 (Data Protection and Encryption) of the Security Overview
Measures for the protection of data during storage	See Section 7.1 (Data Protection and Encryption) of the Security Overview
Measures for ensuring physical security of locations at which personal data are processed	See Section 7.9 (Physical Security) of the Security Overview
Measures for ensuring events logging	See Sections 7.5 (Identity and Access Control), 7.6 (System Development Life Cycle and Application Security), and 8.2 (Logging and Monitoring) of the Security Overview
Measures for ensuring system configuration, including default configuration	See Sections 7.6 (System Development Life Cycle and Application Security), 8 (Detection), and 11.1 (Controls) of the Security Overview
Measures for internal IT and IT security governance and management	See Sections 4 (Security Team) and 6 (Our Staff and Internal Operations) of the Security Overview
Measures for certification/assurance of processes and products	See Section 11 (Certification and Controls) of the Security Overview

Measures for ensuring data minimisation	See Sections 5 (Risks Management), 6 (Our Staff and Internal Operations), and 7 (Prevention) of the Security Overview
Measures for ensuring data quality	See Sections 5 (Risks Management), 6 (Our Staff and Internal Operations), and 7 (Prevention) of the Security Overview
Measures for ensuring limited data retention	See Section 8.2 (Logging and Monitoring) of the Security Overview and Section 8 (Data Retention) of the Privacy Policy
Measures for ensuring accountability	See Sections 2 (Our Commitment to Security) and 11 (Certification and Controls) of the Security Overview and Section 11 (Information for Users in Europe and Elsewhere Outside the U.S.) of the Privacy Policy
Measures for allowing data portability and ensuring erasure	Data subject removal requests can be processed by sending a communication to privacy@zoominfo.com. Deletion of Customer Personal Data shall take place as described in Section 12 of this DPA. Data subject portability requests are supported by ZoomInfo's privacy and security teams. Requests can be sent to privacy@zoominfo.com. Customers may instruct ZoomInfo in writing to return Customer Personal Data as described in Section 12 of this DPA. More information is available within the Privacy Policy in Sections 6 (Your Choices), 8 (Data Retention), and 11 (Information for Users in Europe and Elsewhere Outside the U.S.)
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	When ZoomInfo engages a sub-processor under this DPA, ZoomInfo and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this DPA. Each sub-processor agreement must ensure that ZoomInfo is able to meet its obligations to Customer. See also Section 7.4 (Partners and Vendor Risk) of the Security Overview.

ANNEX III

ZoomInfo’s sub-processors are identified at www.zoominfo.com/legal/subprocessors

<u>**SCHEDULE 2**</u>

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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 when Customer signs the Agreement that incorporates the DPA and this Addendum	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The entity identified as "Customer" or "Licensee" in the Agreement Trading name (if different): Main address (if a company registered address): The contact details associated with Customer's ZoomInfo account or as otherwise specified in the Agreement. Official registration number (if any) (company number or similar identifier):	Full legal name: ZoomInfo Technologies LLC Trading name (if different): ZoomInfo Main address (if a company registered address): 805 Broadway, Suite 800, Vancouver WA 98660 USA Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional); Job Title; and Contact details including email: The contact details associated with Customer's ZoomInfo account or as otherwise specified in the Agreement.	Full Name (optional): James Henry Job Title: Associate General Counsel Contact details including email: legal@zoominfo.com
Signature (if required for the purposes of Section 2)		

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: Date: Reference (if any): Other identifier (if any): Or ☒ 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						
2	X	Omitted	Omitted	General	30 days	
3						
4						

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 1A: List of Parties: See Annex 1A of EU SCCs

Annex 1B: Description of Transfer: See Annex 1B of EU SCCs

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III of EU SCCs

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: ☐ Importer ☐ Exporter ☒ 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 1A 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.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.