DATA PROCESSING ADDENDUM

DPA Effective Date: FEBRUARY 10, 2023 (“DPA Effective Date”)
(formatting, but not content updated on June 28, 2023)

This Data Processing Addendum, including its Schedule and Appendices, ("DPA") supplements the governing document between Licensee with and CB Information Services, Inc., with offices in New York City, United States of America (“CBI” or “Licensor”), effective as of the date of signature and all ordering documents (collectively, “Agreement”) pertaining to the processing of Personal Data as related to the Agreement. To the extent of any conflict or inconsistency between the provisions of the body of the DPA and the Agreement, the terms of the DPA shall prevail. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.
In the course of providing the Services to Licensee pursuant to the Agreement, CBI may Process Personal Data on behalf of Licensee and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

PROCESSING OF PERSONAL DATA

1. Scope and Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Licensee is the Controller, CBI is the Processor and that CBI will engage Sub-processors pursuant to the requirements set forth in Section 4 (“Sub-processors”) below.
2. Licensee's Processing of Personal Data. Licensee shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of CBI as Processor. For the avoidance of doubt, Licensee's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Licensee shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Licensee acquired Personal Data. Licensee specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.
3. CBI's Processing of Personal Data. CBI shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Licensee's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Licensee (e.g., via email) where such instructions are consistent with the terms of the Agreement. Additionally, CBI shall:
    a. only act on the written instructions of Licensee (unless required by law to act without such instructions);
    b. ensure that people processing the Personal Data are subject to a duty of confidence;
    c. take appropriate technical and organizational measures to ensure that the security of Processing is appropriate to the risk, taking account of the state of the art, the costs of implementation, and the nature, scope, context and purpose of the Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons;
    d. assist Licensee in meeting its GDPR obligations in relation to the security of Processing, the notification of Licensee Data Incidents (as defined herein), prior consultation with the relevant GDPR supervisory authority, and data protection impact assessments; and
    e. submit to reasonable audits; provide Licensee with reasonable information it needs to ensure that both

parties are meeting obligations under the GDPR; and inform Licensee immediately if asked to act in any way infringing the GDPR or other Data Protection Laws and Regulations

4. Details of the Processing.

    a. Subject Matter: User access of the Services.

    b. Duration: the duration of the Agreement.

    c. Purpose: provision of the Services, initiated by Users.

    d. Nature of the Processing: Personal Data to be processed at User login and sent to CBI's authentication server (Amazon Web Services servers), which Personal Data is used to find the encrypted password and match with User's entered credentials. Personal Data and non-identifying ID stored on the server for the duration of the login session.

    e. Type of Personal Data: Email addresses (including name) and IP addresses at User login.

    f. Categories of Data Subjects: Users, which are limited to Licensee's and its Affiliates' employees or agents, who have an email address with Licensee or its Affiliates and have access to the Services under an Order Form.

RIGHTS OF DATA SUBJECTS. CBI shall, to the extent legally permitted, promptly notify Licensee if CBI receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request." Taking into account the nature of the Processing, CBI shall assist Licensee by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Licensee's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Licensee, in its use of the Services, does not have the ability to address a Data Subject Request, CBI shall upon Licensee's request provide commercially reasonable efforts to assist Licensee in responding to such Data Subject Request, to the extent CBI is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Licensee shall be responsible for any costs arising from CBI' s provision of such assistance.

CBI PERSONNEL AND CONFIDENTIALITY. BI shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. CBI shall ensure that such confidentiality obligations survive the termination of the personnel engagement. CBI shall take commercially reasonable steps to ensure the reliability of any CBI personnel engaged in the Processing of Personal Data. CBI shall ensure that CBI's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

SUBPROCESSORS. Licensee acknowledges and agrees that, to the extent applicable, (a) CBI's Affiliates may be retained as Subprocessors; and (b) CBI and CBI's Affiliates respectively may engage appropriate third-party Sub-processors in connection with the provision of the Services. CBI shall promptly and no later than 14 days from the date of this DPA, provide Licensee with a list of all Sub-processors appointed in accordance with this clause 4. CBI shall give Licensee reasonable notice in writing of any proposed change of Sub-processors. CBI has entered into, or shall enter into as necessary in each instance, a written agreement with each Sub- processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Licensee Data to the extent applicable to the nature of the Services provided by such Sub-processor. CBI shall be liable for the acts and omissions of its Sub-processors to the same extent CBI would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

SECURITY. CBI shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized

disclosure of, or access to, Licensee Data), confidentiality and integrity of Licensee Data. CBI regularly monitors compliance with these measures. CBI will not materially decrease the overall security of the Services during a Subscription Term.

LICENSEE DATA INCIDENT MANAGEMENT AND NOTIFICATION. CBI shall notify Licensee without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Licensee Data, including Personal Data, transmitted, stored or otherwise Processed by CBI or its Sub-processors of which CBI becomes aware (a "Licensee Data Incident"). CBI shall make reasonable efforts to identify the cause of such Licensee Data Incident and take those steps as CBI deems necessary and reasonable in order to remediate the cause of such a Licensee Data Incident to the extent the remediation is within CBI's reasonable control. The obligations herein shall not apply to incidents that are caused by Licensee or Licensee' s Users.

DELETION OF LICENSEE DATA. CBI shall, except to the extent CBI is required by applicable law to retain Licensee Data and where CBI has given Licensee prior written notice of such requirement of law, promptly return or otherwise at Licensee's request, delete (providing Licensee with written evidence thereof) all Licensee Data and copies thereof.

AUTHORIZED AFFILIATES

1. Contractual Relationship. The parties acknowledge and agree that, by executing this DPA, Licensee enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between CBI and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Licensee.
2. Communication. The Licensee that is the contracting party to the Agreement shall remain responsible for coordinating all communication with CBI under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.
3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with CBI, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:
    a. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against CBI directly by itself, the parties agree that (i) solely the Licensee that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Licensee that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in Section 8.3.2, below).
    b. The parties agree that the Licensee that is the contracting party to the Agreement shall, when carrying out an on• site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on CBI and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

LIMITATION OF LIABILITY. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and CBI, whether in contract, tort, or under any other theory of liability, is subject to the Limitation of Liability section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, CBI's and its Affiliates' total liability for all claims from Licensee and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall

apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Licensee and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Licensee and/or to any Authorized Affiliate that is a contractual party to any such DPA.

TRANSFER OF PERSONAL DATA. The Standard Contractual Clauses will apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if CBI has adopted or does adopt binding corporate rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
"Authorized Affiliate" mean s any of Licensee's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and /or the Uni ted Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Licensee and CBI, but has not signed its own Order Form with CBI and is not a "Licensee" as defined under this DPA.
"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code§ 1798.100 *et seq.,* and its implementing regulations.
"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.
"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement.
"Data Subject" means the identified or identifiable person to whom Personal Data relates. For purposes of this DPA, Data Subjects shall primarily be limited to Users of the Services.
"EEA" means the European Economic Area.
"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protect ion Regulation) and the Data Protection Act 2018.
"Licensee" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.
"Licensee Data" means what is defined in the Agreement as "Licensee Data," provided that such data is electronic data and information submitted by or for Licensee to the Services.
"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Licensee Data.
"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.
"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.
"Standard Contractual Clauses" means the agreement executed by and between Licensee and CB Information Services, Inc. and attached hereto as Schedule 1 pursuant to the European Commission's decision of 5-February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
"Subprocessor" means any Processor engaged by CBI.

SCHEDULE 1 - STANDARD CONTRACTUAL CLAUSES

Clause 1
Definitions
For the purposes of the Clauses:

1. *'personal data ', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

2. *'the data exporter'* means the controller who transfers the personal data;

3. *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country ' s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

4. *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

5. *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established ;

6. *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer
The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to U), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data expo1ier and the importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter
The data exporter agrees and warrants:

1. that the process i ng, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
2. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
5. that it will ensure compliance with the security measures;
6. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
7. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures , as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
9. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
10. that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer
The data importer agrees and warrants:

1. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses ; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
    a. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
    b. any accidental or unauthorised access, and
    c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
5. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
6. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial in formation, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
8. that, in the event of subprocess in g, it has previously informed the data exporter and obtained its prior written consent;
9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
10. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law
The Clauses shall be governed by the law of the Member State in which the data exporter is established.
Clause 10
Variation of the contract
The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.
Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The Clauses shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data

exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
The data exporter is the entity identified as "Licensee" in the DPA

Data importer
The data importer is CB Information Services, Inc., a provider of an online database providing data on private companies and emerging technologies, and accompanying research regarding the same.

Data subjects
Data subjects are defined in Section 1.4 of the DPA.

Categories of data
The personal data categories are defined in Section 1.4 of the DPA.

Processing operations
The processing operations are defined in Section 1.4 of the DPA

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES
This Appendix forms part of the Clauses and must be completed by the parties
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Users are required to log in over SSL. Login submissions are encrypted upon submission. Passwords are salted and hashed when stored in the database.
Personal user data is stored in a separate database to platform data with different access credentials.

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services. Data Importer will not materially decrease the overall security of the SCC Services during a subscription term.

Information Security Program. CBI maintains and will continue to maintain an information security program, adopting and enforcing internal policies and procedures necessary to: (a) help Licensee secure Personal Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to any of CBI's servers, networking equipment, and other related systems ("CBI Network"), and (c) minimize security risks, including through risk assessment and regular testing. CBI will designate one or more employees to coordinate and be accountable for the information security program.

The information security program will include the following measures.

Network Security. The CBI Network is accessible to employees, contractors, and other persons only as necessary to provide the Services. CBI maintains and will maintain access controls and policies to determine and manage access permission to the CBI Network from each network connection and user, inclusive of firewalls or functionally equivalent technology and authentication controls. CBI maintains or will maintain corrective action and incident response plans to respond to potential security threats.

Limited Access. CBI provides access to the CBI Network to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to them, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of CBI.

CBI Physical Security. Although most of the Services are hosted on certain AWS Networks in AWS Facilities (as defined below, respectively). Physical components of the CBI Network are housed in the CBI office ("CBI Offices"). Physical barrier controls are used to prevent unauthorized entrance to the CBI Offices both at the building entrance and at building access points. Passage through the physical barriers at the CBI Offices requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel. CBI employees and contractors are assigned photo-ID badges that must be carried within the CBI Offices. Visitors are required to sign-in with designated personnel, must show appropriate identification. Access points to the CBI Offices are monitored by video surveillance cameras designed to record all individuals accessing the CBI Offices. CBI also maintains electronic intrusion detection systems designed to detect unauthorized access to the CBI Offices.

Continued Evaluation. CBI will conduct periodic reviews of the security of the CBI Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. CBI will continually evaluate the security of the CBI Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

AWS Physical Security. In addition to the CBI Network, the Services are hosted on certain AWS data center facilities, servers, networking equipment, and host software systems all located in the United States (e.g., virtual firewalls) and which are within AWS's control ("AWS Network"). Physical components of the AWS Network are housed in nondescript facilities ("AWS Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the AWS Facilities both at the perimeter and at building access points. Passage through the physical barriers at the AWS Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). AWS employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the AWS Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the AWS Facilities, and are continually escorted by authorized employees or contractors while visiting the AWS Facilities. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the AWS Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the AWS Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the AWS Facilities by AWS employees and contractors is logged and routinely audited.