DATA PROCESSING AGREEMENT

Last updated July 3, 2023

This Data Processing Agreement (the "DPA") available at https://legal.cbinsights.com/ forms part of and is incorporated into the Agreement or other written or electronic agreement (the "Agreement") between Customer and CB Information Services, Inc. ("CB Insights"). Each of CB Insights and Customer shall be referred to individually as a Party and collectively as the Parties. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

As specifically indicated in the Agreement, Customer enters into this DPA on behalf of itself and on behalf of its Affiliates to the extent CB Insights processes Personal Data on behalf of Customer and its Affiliates in the course of providing Services.

In order to enable the Parties to carry out their relationship in a manner that is compliant with Applicable Data Protection Law, the Parties agree follows:

1.DEFINITIONS

All terms and phrases not defined herein shall have the meanings set forth in the Agreement or in Applicable Data Protection Law.

"Affiliate" means any Customer affiliate permitted to use the Services pursuant to the Agreement.

"Applicable Data Protection Law" means the laws and regulations applicable to the Processing of Personal Data under the Agreement.

"California Privacy Laws" means the California Consumer Privacy Act of 2018, as amended the California Privacy Rights Act of 2020, and their respective implementing regulations.

"Controller" and "Business" means the party that determines the purposes and means of the Processing of Personal Data.

"Customer" means the entity that executed the Agreement together with its Affiliates, which Affiliates have signed an Order Form.

"Customer Data" means any and all information provided or made available by Customer to CB Insights through Customer's access to and use of the Services.

"Data Subject" means an identified or identifiable person entitled to rights under Applicable Data Protection Law and to whom Personal Data relates.

"GDPR" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"Personal Data"means any information relating to an identified or identifiable natural person where such information is protected as personal data, personal information, or personally identifiable information under Applicable Data Protection Law where such data is Customer Data.

"Processing" means an 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, and whereas "Process," "Processes," and "Processed" shall be interpreted accordingly.

"Processor" and "Service Provider" mean a Party that Processes Personal Data on behalf of a Controller.

"Security Breach" means a breach of security of the CB Insights security standards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"Services" means the Services, including any customer support services, provided by CB Insights to Customer pursuant to the

Agreement.

"Standard Contractual Clauses" shall mean (i) the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, as may updated, amended, and superseded from time-to-time; and (ii) and the UK International Data Transfer Addendum ("UK IDTA") available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may updated, amended, and superseded from time-to-time.

"Sub-processor"means any third party engaged by CB Insights that Processes Personal Data.

"Supervisory Authority"means an applicable independent public authority which is established by an EU Member State pursuant to the GDPR, the UK Information Commissioner's Office (ICO), or the Swiss Federal Data Protection and Information Commissioner (FDPIC).

"UK GDPR" means the Data Protection Act 2018, including any amendments thereto.

2. DATA PROCESSING TERMS

2.1 Roles and Relationships. The Parties acknowledge and agree that with regard to Personal Data Processed under the Agreement, Customer is the Controller and CB Insights is the Processor. With respect to the California Privacy Laws, CB Insights shall be considered a Service Provider to Customer, which is the Business, to the extent that the California Privacy Laws apply.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services and provision of instructions to CB Insights, process Personal Data in accordance with Applicable Data Protection Law. Customer is solely responsible for its compliance with Applicable Data Protection Law, including providing required notices and obtaining required consents, and in regards to the accuracy, quality, and lawful basis of Processing and the means by which Customer acquired such Personal Data with respect to Customer's use of the Services.

2.3 Documented Instruction. Customer instructs CB Insights to process Personal Data for the purposes of providing the Services in accordance with the Agreement and any other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

2.4 Details of Processing. The subject matter of the Processing is the Services under the Agreement, the nature of which Processing is as set forth in the Agreement. The duration of Processing shall be for the duration of the provision of Services to Customer and any time thereafter as may be expressly agreed by CB Insights and Customer or as may be permitted or required by applicable law.

2.5 California Privacy Laws. For purposes of the California Privacy Laws, the nature of the Processing is for a Business Purpose and does not involve the "sale" or "sharing" of Personal Data by CB Insights, as such term is defined by the California Privacy Laws. CB Insights shall not retain, use, or disclose Personal Data for any purpose other than for the Business Purpose specified in the Agreement and shall not combine Personal Data with other information except as expressly permitted by Customer or the California Privacy Laws. CB Insights shall comply with the obligations of and provide the same level of protection as required by the applicable California Privacy Laws. As set forth in Section 3.5, CB Insights grants Customer the right, upon notice, to take reasonable and appropriate steps to help ensure that CB Insights uses the Personal Data in a manner consistent with the California Privacy Laws and to stop and remediate the unauthorize use of Personal Data. CB Insights will cooperate with Customer in responding to verifiable consumers requests, such as in regards to the deletion of Personal Data. CB Insights will notify Customer if it determines that it can no longer meet its obligations under the California Privacy Laws.

3.PROCESSOR OBLIGATIONS

3.1 Confidentiality. Persons authorized by CB Insights to Process Personal Data shall be committed to a duty of confidentiality.

3.2 Processing Limitations. CB Insights shall process Personal Data in accordance with Customer's documented instructions and/or as otherwise permitted or required by Applicable Data Protection Law. CB Insights shall immediately inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

3.3 Security of Processing. CB Insights shall implement the technical and organizational measures, as set out in Annex II to the

Standard Contractual Clauses attached to this DPA, designed to protect against the unauthorized or unlawful processing, accidental or unlawful destruction, loss or alteration or damage, and unauthorized disclosure or access to Personal Data.

3.4 Security Breach Notification. CB Insights shall notify Customer without undue delay upon becoming aware of a breach of Personal Data for which notification to Customer is required under Applicable Data Protection Law. To the extent that the cause of the breach of Personal Data can be reasonably mitigated by CB Insights, CB Insights shall use commercially reasonable efforts to mitigate such cause.

3.5 Audits and Inspections. Upon Customer's reasonable request and subject to the confidentiality obligations set forth in the Agreement, CB Insights shall make available to Customer a copy of CB Insights' then most recent third-party audits or certifications, to the extent applicable and available (the "Audit Report") subject to CB Insights' redaction of information reasonably determined by CB Insights to constitute "High Sensitivity" information. To the extent that additional information is necessary to satisfy Customer's audit requirements under Applicable Data Protection Law, upon not less than thirty (30) days' notice and at Customer's expense, and not more frequently than once per 12-month period (unless required by Applicable Data Protection Law), Customer may request such additional information, up to and including remote inspections of the systems and processes involved in the Processing of Personal Data. Remote audits shall be performed in a manner that limits disruption to CB Insights' business operations and in accordance with CB Insights' security policies. CB Insights shall comply, as legally necessary, with audits by a competent Supervisory Authority (or other competent regulator of Personal Data) under Applicable Data Protection Law.

3.6 Data Subject Rights. Taking into account the nature of the processing and to the extent Customer cannot respond to a Data Subject request through functionality made available via the Services, CB Insights shall provide commercially reasonable assistance upon Customer's request to enable Customer to fulfill its obligations with respect to responding to Data Subject requests under Applicable Data Protection Law.

3.7 Data Protection Impact Assessments and Prior Consultation. To the extent required by Applicable Data Protection Law in relation to the Processing of Personal Data by CB Insights, CB Insights shall render reasonable assistance to Customer in performing Data Protection Impact Assessments and providing Prior Consultation in accordance with Applicable Data Protection Law. CB Insights reserves the right to charge Customer for its reasonable expenses in providing such assistance.

3.8 Return or Deletion of Personal Data. As may be required by Applicable Data Protection Law, upon termination of the Services, CB Insights shall, upon Customer's written request and/or as may be provided in the Agreement, return or delete Personal Data, including copies of such data in CB Insights' custody or control, unless and only to the extent CB Insights has a legitimate legal basis for retaining such data. With respect to deletion, CB Insights shall utilize a commercially reasonable means of deletion and/or disposal of its choosing. If CB Insights retains Personal Data for legal reasons, CB Insights will only actively process such Personal Data in accordance with applicable law. Notwithstanding the foregoing, CB Insights may retain any anonymous information obtained through Customer's use of the Services.

4.SUBPROCESSING

4.1 Appointment of Sub-processors. CB Insights may appoint and retain Sub-processors, which may include its Affiliates, in the Processing of Personal Data. Customer further agrees CB Insights' Sub-processors may engage Sub-processors in the Processing of Personal Data. CB Insights shall remain responsible for the acts and omissions of its Sub-processors as for its own acts and omissions. Sub-processors shall be bound to Processing Personal Data consistent with the requirements hereunder and Applicable Data Protection Law.

4.2 General Authorization. CB Insights shall have Customer's general authorization to engage Sub-processors from the Sub-processor List available here https://legal.cbinsights.com/, as may be updated from time-to-time.

4.3 Change in Sub-processors. CB Insights may remove, replace, and appoint new Sub-processors in its discretion upon ten (10) days written notice, which notice may be provided through CB Insights' updating its Sub-processor List at https://legal.cbinsights.com/. Customer may object in writing to the appointment of a new Sub-processor on grounds of data protection within ten (10) days of CB Insights' notice of such appointment, otherwise the appointment shall be deemed accepted by Customer. Any objection by Customer to the appointment of a Sub-processor shall be made in good faith and supported by reasonable information. Upon Customer making such an objection, CB Insights and Customer shall negotiate in good faith to reach a mutually agreeable resolution within thirty (30)

days of CB Insights' receipt of Customer's objection. If a resolution cannot be reached within thirty (30) days of CB Insights' receipt of Customer's objection, either Party may terminate the affected portion of the Services without further liability upon reasonable written notice.

5.AFFILIATES

5.1 Contractual Relationship. The Parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA in the name of and on behalf of itself and, as applicable, its Affiliates, thereby establishing a separate DPA between CB Insights and each such Affiliate subject to the provisions of the Agreement. Each Affiliate agrees to be bound by this DPA.

5.2 Communications. Customer, as the contracting party to the Agreement, is solely responsible for coordinating all communications with CB Insights under this DPA and making and receiving any communications in relation to this DPA on behalf of its Affiliates.

5.3 Rights of Affiliates. Where an Affiliate becomes a party to this DPA, it shall to the extent required under Applicable Data Protection Law be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

> Except where applicable Data Protection Law requires the Affiliate to exercise a right or seek any remedy under this DPA against CB Insights directly, the Parties agree that (i) Customer shall exercise any such right or seek any such remedy on behalf of the Affiliate, and (ii) Customer shall exercise any such right under this DPA not separately for each Affiliate individually but in a combined manner for itself and all of its Affiliates together.

6.TRANSFERS TO THIRD COUNTRIES

This Section 6 applies only if and to the extent that Personal Data Processed under the Agreement is transferred to a third country from the European Union/European Economic Area ("EU/EEA"), United Kingdom ("UK"), and/or Switzerland, not subject to an applicable adequacy decision.

6.1 Incorporation and Application of Standard Contractual Clauses. This DPA incorporates by reference the Standard Contractual Clauses for international transfers of Personal Data from the EU/EEA, UK, and Switzerland, respectively, as permissibly customized by the Parties. The Standard Contractual Clauses shall apply only if and to the extent Personal Data Processed under the Agreement is subject to a restriction on such transfer (e.g., a transfer not covered by an adequacy decision) under the GDPR, UK GDPR, or FADP (a "Restricted Transfer").

To the extent that the Standard Contractual Clauses apply, the Standard Contractual Clauses shall prevail over contradictions between this DPA and the Standard Contractual Clauses with respect to the subject matter of the Standard Contractual Clauses.

Where Personal Data is subject to a Restricted Transfer from Switzerland, the Standard Contractual Clauses shall be modified in accordance with the following:

(a) "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.

(b) "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 September 2023.

(c) The term "EU Member State" are not to be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

(d) The Standard Contractual Clauses shall also protect the data of legal entities until the entry into force of the Revised FADP.

(e) The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

6.2 Invalidation Event. In the event that the Standard Contractual Clauses are invalidated, replaced, superseded, or otherwise determined by an applicable competent authority to no longer provide adequate protection to a transfer of Personal Data to a relevant third country or countries (an "Invalidation Event"), the Parties agree to reasonably cooperate to adopt another appropriate transfer mechanism to prevent undue disruptions to the transfers of Personal Data to such third country or countries.

6.3 Transfer Impact Assessment. To the extent required by Applicable Data Protection Law, the Parties agree to reasonably cooperate to assess the risks associated with Restricted Transfers of Personal Data. The Parties agree that such assessment(s) shall be

Confidential Information provided that disclosure to the Supervisory Authority is permitted by either Party upon the Supervisory Authority's legitimate request for such information.

7.GENERAL TERMS

7.1 Term and Termination. The term of this DPA is identical to the term of the Agreement. Except as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.

7.2 Governing Law and Dispute Resolution. Governing law and dispute resolution shall be the same as set forth in the Agreement.

7.3 Notice. Any and all notices shall made be as set forth in the Agreement.

7.4 Amendment. This DPA may be amended from time-to-time by CB Insights in its sole discretion upon thirty (30) days' notice to Customer.

7.5 Entire Agreement. This DPA constitutes the entire agreement between the Parties hereto with respect to the subject matter hereof and supersedes any and all prior written and/or oral agreements.

Schedule to the DPA

1. With respect to the EU/EEA Standard Contractual Clauses Annexes I, II, and III, the following shall apply:

Controller/Exporter	Customer, as set forth in the Agreement
Processor/Importer	CB Insights, as set forth in the Agreement
Date of the Clauses	As of the date of the Agreement
Module	Module Two: Transfer Controller to Processor
Data Controller/Exporter is engaged in	Consumption of the specified Services under the Agreement
Data Controller/Exporter is using the personal data which is being transferred for the following purposes or activities	CB Insights' specified Services under the Agreement
Data Processor/Importer is engaged in	The provision of the Services specified in the Agreement
Categories of data subjects	The data subjects are those who are the object of the Processing set forth in the

	Agreement, namely Customer's designated end users of the Services
Categories of personal data	Controller/Exporter determines and controls, in its sole discretion, the information transferred by and through its consumption of the Services or as otherwise provided to CB Insights.
Sensitive or special category data	n/a
Frequency of the transfer	Continuous per Customer's consumption of the Services
Nature of the processing	Data Processor/Importer will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Data Controller/Exporter in its use of the Services. Consistent with the Services, processing operations include receiving data, collection, accessing, retrieval, recording, and data entry; holding data, including storage, organisation and structuring; and using data, including analysing and testing.
Purpose of the data transfer and further processing	To Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Controller/Exporter in its use of the Services
Retention period (or criteria used to determine retention)	Personal Data is retained for the period of the Agreement unless otherwise retained for legal or compliance purposes or as otherwise permitted by Applicable Data Protection Law
For the purposes of Clause 7	Docking Clause is included
For the purpose of Clause 9(a), use of sub-processors, the data importer has the Data Controller's/Exporter's	General written authorization for the engagement of sub-processors in accordance with Section 4 of the DPA
For the purposes of the Clause 9(a), the Data Processor/Importer shall specifically inform the Data Controller/Exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least	Ten (10) days in advance, in accordance with Section 4 of the DPA

For the purposes of Clause 11, Redress	Option concerning redress with an independent dispute resolution body is not included
For the purposes of Clause 13, the competent supervisory authority is	Republic of Ireland
For the purposes of Clause 17, governing law shall be the law of the	Republic of Ireland
For the purposes of Clause 18, choice of forum and jurisdiction shall be the	Republic of Ireland
Technical and organisational measures including technical and organisational measures to ensure the security of the data	The technical and organization measures set forth in Annex II to the Standard Contractual Clauses (Appendix I to the DPA)

2. With respect to the UK International Data Transfer Addendum to the EU/EEA Standard Contractual Clauses (the "UK IDTA") Tables 1 through 4, the following shall apply:

Table 1: Parties

Start Date	As of the date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer
Parties' details	Customer, as set forth in the Agreement	CB Insights, as set forth in the Agreement
Key Contact	As set forth in the Agreement, or as provided to CB Insights upon request	As set forth in the Agreement, or as provided to Customer upon request

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ the Approved EU SCCs, including the Appendix Information and with only the above modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.

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: as set out in section (1) of the Schedule to the DPA

Annex 1B: Description of Transfer: as set out in section (1) of the Schedule to the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as set out in Annex II to the Standard Contractual Clauses attached to the DPA

Annex III: List of Sub processors (Modules 2 and 3 only): as set out in Annex III to the Standard Contractual Clauses attached to the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	☒ Importer ☒ Exporter

APPENDIX I

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition,

the data may only be disclosed to a third party located outside the European Union *(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.

(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.

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 ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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.

(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.

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 to 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 set forth in the Schedule to the DPA.

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 set forth in the Schedule to the DPA.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): As set forth in the Schedule to the DPA

Data importer(s): As set forth in the Schedule to the DPA

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set forth in the Schedule to the DPA

Categories of personal data transferred

As set forth in the Schedule to the DPA

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.

N/A

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

As set forth in the Schedule to the DPA

Nature of the processing

As set forth in the Schedule to the DPA

Purpose(s) of the data transfer and further processing

As set forth in the Schedule to the DPA

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

As set forth in the Schedule to the DPA

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

See DPA and list of sub-processors at https://legal.cbinsights.com/

C. COMPETENT SUPERVISORY AUTHORITY

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

As set forth in the Schedule to the DPA

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.

Network and Access Security. 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 Data of users 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.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has granted the processor general authorization to engage sub-processors. Such sub-processors are set forth here https://legal.cbinsights.com/, which list may be updated from time-to-time pursuant to Section 4 of the Data Processing Agreement.

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

As set forth in the Schedule to the DPA.

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 IA 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	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data

Safeguards	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.