DATA PROCESSING ADDENDUM

Revised: March 15, 2024

See previous versions here: https://www.bmc.com/legal/data-processing-addendum.html

This Data Processing Addendum ("**DPA**") supplements and forms part of the Master Services Agreement or other written agreement for subscription and/or purchase of services and/or products by BMC, as such Services are described in the corresponding Order(s) and/or Statement of Work(s) attached to such Agreement(s) (collectively the "**Agreement(s)**") executed by the entity set forth in the signature block of the Agreement ("**Company**") and the BMC entity set forth in the signature block of the Agreement ("**BMC**"). Company and BMC may be referred to individually as a "**Party**" or collectively as the "**Parties**". Any capitalized terms that are undefined in this DPA will have the definitions set forth in the Agreement.

BMC and Company's signature on the Agreement shall constitute signature and acceptance of this DPA and the Standard Contractual Clauses and their Appendices (as populated by the information located in the Agreement, DPA, and its Exhibits) to the extent that the Standard Contractual Clauses are applicable and required for the lawful transfer and Processing of Personal Data.

BMC is committed to complying with applicable data protection laws ("**Data Protection Laws**"), including (i) Regulation 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 ("**GDPR**"), and (ii) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as incorporated into and amended by the European Union (Withdrawal) Act 2018 as amended or superseded from time to time ("**UK Data Protection Laws**").

SECTION 1. INCORPORATION OF RELEVANT DATA PROTECTION PROVISIONS

The Section modifies and/or replaces previous data protection provisions of the existing Agreement(s) between Company and BMC:

1. Definitions.

1.1 For the purposes of this Agreement, the terms "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Breach**", "**Data Protection Impact Assessment**", "**Prior Consultation**", "**Data Subject**", "**Transfer**", "**Appropriate Safeguards**" and "**Supervisory Authority**" shall have the meaning given to them by Data Protection Laws.

1.2 **"Data Protection Laws"** means any applicable data protection laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data, including (i) Regulation 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 (**"EU GDPR"**); (ii) the UK Data Protection Act 2018; (iii) the UK General Data Protection Regulation as incorporated into and amended by the European Union (Withdrawal) Act 2018 as amended or superseded from time to time ("**UK GDPR**"); (iv) the California Consumer Privacy Act ("**CCPA**"); and (v) the Swiss Federal Act on Data Protection; in each case, as updated, amended or replaced from time to time.

1.3 "**Standard Contractual Clauses**" or "**SCCs**" means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, and any amendments to, or replacements of, those clauses (**"EU SCCs"**); and (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses approved by the UK Information Commissioner's Office, and any amendments to, or replacements of, that addendum ("**UK Addendum**").

1.4 "**Sub-Processor**" means any other data Processor engaged by a Processor for carrying out specific activities on behalf of the Controller.

2. Roles of the Parties.

2.1 This DPA reflects the parties' commitment to abide by Data Protection Laws when Processing BMC Personal Data pursuant to the Agreement. In the course of the subscription and/or purchase of the Services by BMC from Company pursuant to the Agreement(s), Company may have access to BMC's Personal Data as may be submitted to Company by BMC. Both BMC and Company shall fulfill their respective legal obligations under Data Protection Laws.

2.2 The Parties acknowledge and agree that BMC determines the purposes and means of the Personal Data Processing activities performed by Company to deliver the Services under this Agreement and shall be considered the Controller. Company processes Personal Data on behalf of BMC and shall be considered the Processor.

2.3 The Parties acknowledge and agree that when the purposes and means of the Personal Data Processing activities are determined by BMC's client, BMC's client shall be considered the Controller, BMC shall be considered the Processor and Company shall be considered the Sub-Processor.

2.4 The Personal Data Processing activities in scope of this Agreement are specified in Exhibit 1 of the Agreement.

3. **BMC Data Protection Binding Corporate Rules.** BMC adheres to its (i) Controller and Processor EU Binding Corporate Rules Policy, and (ii) Controller and Processor UK Binding Corporate Rules Policy, (together the "**BCR**"), with respect to compliance with Data Protection Laws. A copy of the BCR can be found on www.bmc.com. The BCR require BMC to contractually ensure that its Processors and Sub-Processors adopt and comply with appropriate and equivalent Data Protection obligations. Such Data Protection obligations are reflected in this DPA.

4. **Instructions.** Company shall only process Personal Data for the purpose of fulfilling its obligations under the Agreements, according to BMC documented instructions and applicable Data Protection Laws. Company shall immediately inform BMC if, in the Company's opinion, an instruction from BMC may infringe Data Protection Laws. Company shall not process Personal Data except on instructions from BMC, unless required to do so by Data Protection Laws. In particular, Company shall not include Personal Data in any product or service offered by Company to third parties or carry out any further research, analysis or profiling activity which involves the use of any element of the Personal Data (including in aggregate form) or any information derived from any processing of such Personal Data outside the scope of the Services without BMC's prior authorization.

5. **Security.** Company shall maintain appropriate technical and organizational protection measures in accordance with the Information Security Requirements set forth at https://www.bmc.com/documents/various/information-security-requirements.html ("**Information Security Requirements**"). Company shall regularly monitor compliance with these measures.

6. **Limited Access and Confidentiality.** Personal Data shall be made available only to Company's personnel that require access to such Personal Data for the performance of the Services. Company shall ensure that all its personnel having access to Personal Data have committed themselves to confidentiality by executing written confidentiality obligations. The obligation to treat Personal Data pursuant to such confidentiality obligations shall survive the termination of the employment.

7. **Sub-Processing.**

7.1 BMC generally acknowledges and agrees that Company may engage third parties as Sub-Processors in connection with the Services, including access to Personal Data. Sub-Processors shall be obliged under a written contract (i) to comply with Data Protection Laws and (ii) to provide the same data protection obligations as set out by this Agreement, including the implementation of appropriate technical and organizational measures.

7.2 A full list of all Sub-Processors as of the Effective Date of this Agreement is provided in Exhibit 1 of the Agreement. Any additions or replacements of Sub-Processors shall be notified to BMC via email. BMC may oppose to Company use of a new Sub-Processor by notifying Company in writing of its objective reasons to oppose within thirty (30) business days after receipt of Company's notice. In the event BMC objects to a new Sub-Processor, Company shall use reasonable efforts to make available to BMC a change in the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening BMC. If Company is unable to make available such change within a reasonable period of time, BMC may terminate the Agreement(s) with respect only to those Services which cannot be provided by Company without the use of the objected-to new Sub-Processor by providing written notice to Company shall refund BMC any prepaid fees covering the remainder of the term of the Agreement(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on BMC.

7.3 Where a Sub-Processor would fail to fulfil its data protection obligations under this Section, Company shall remain fully liable to BMC for the performance of that Sub-Processor's obligations.

7.4 BMC may require the Company by notice in writing to cease or suspend the processing of Personal Data by a Sub-Processor if, in the reasonable opinion of BMC, the Sub-Processor is processing Personal Data in breach of this Agreement.

8. **Assistance to BMC**

8.1 If Company receives a request from a Data Subject to exercise the Data Subject's (a) right of access, (b) right to rectification, (c) restriction of Processing, (d) erasure ("right to be forgotten"), (e) data portability, (f) object to the

Processing, or (g) not to be subject to an automated individual decision making ("**Data Subject Request**"), Company shall notify BMC no later than 5 (five) business days after receiving the request. Such notifications shall be sent to privacy@bmc.com. To the extent BMC, in its use of the Services, does not have the ability to address a Data Subject's request, Company shall provide reasonable assistance and cooperation to BMC in responding to such request. Company shall be responsible for any cost arising from Company's provision of such cooperation and assistance.

8.2 Upon BMC's request, Company shall provide BMC with reasonable cooperation and assistance to fulfill BMC's obligation under Data Protection Laws to implement and maintain appropriate technical and organizational protection measures, insofar as this obligation relates to the Services in scope of this Agreement.

8.3 Upon BMC's request, Company shall provide BMC with reasonable cooperation and assistance to fulfil BMC's obligation under Data Protection Laws to notify a Personal Data Breach to the Supervisory Authority and to communicate on a Personal Data Breach to the Data Subject, insofar as this obligation relates to the Services in scope of this Agreement.

8.4 Upon BMC's request, Company shall provide BMC with reasonable cooperation and assistance to fulfil BMC's obligation under Data Protection Laws to carry out a Data Protection Impact Assessment related to BMC's use of the Services, to the extent BMC does not otherwise have access to the relevant information. Company shall provide reasonable cooperation and assistance to BMC in the Prior Consultation with the competent Supervisory Authority.

9. Data Retention, Deletion and Return.

9.1 To the extent BMC, in its use of the Services, does not have the ability to delete or anonymize Personal Data, Company shall delete, return, or anonymize Personal Data as per BMC instructions.

9.2 Upon BMC's request made within thirty (30) days after the effective date of termination of the Agreement, Company shall make available to BMC for download a file of Personal Data in comma separated value (.csv) format or database backup format. After such 30-day period and except agreed otherwise with BMC, Company shall delete Personal Data from the Services, including copies, unless legally prohibited. In the event Company is unable to delete all or part of BMC Personal Data past such 30-day period for any other reason than a legal prohibition, Company expressly acknowledges and agrees that such processing will not be performed in accordance with BMC's instructions, but for Company's own purposes because of Company's technical inability to delete all BMC Personal Data within the specified timeframe. In such case, Company will act as a Controller of such Personal Data it is processing and remain liable for such Personal Data until it is deleted its systems. Company will provide a letter from an officer of the company certifying the destruction of such data using the template attached as Exhibit 1 of the DPA.

10. Compliance Documentation and Audit Rights.

10.1 Upon BMC's request and to the extent reasonably required, Company shall make available to BMC all relevant information necessary to demonstrate compliance with this DPA ("**Compliance Documentation**"), and allow for and contribute to audits, including inspections, by BMC or an auditor mandated by BMC in relation to the Processing of the BMC Personal Data by Company and its Sub-Processors, provided that BMC shall: (i) give not less than 30 days' written notice in advance of any audit or inspection to be conducted; (ii) shall make reasonable endeavors to avoid causing any damage or disruption to Company's premises, equipment, and business while its personnel are on those premises in the course of such an audit or inspection. Any audit shall not be carried out more than once a year. Any access to Company's premises for the purposes of such an audit or inspection is subject to: (a) the production of reasonable evidence of identity and authority by the auditors; (b) normal business hours; (c) audit personnel have committed themselves to confidentiality by executing written confidentiality obligations; and (d) access only to information that is strictly relevant to the Services provided to BMC. In the event such audit or inspection reveals a material breach of this DPA, Company shall be responsible for any reasonable costs arising from such audit.

10.2 Company acknowledges and agrees that when Company acts as a Sub-Processor of BMC's clients, such BMC Clients may perform audits of Company and Company's Sub-Processors to confirm compliance with this DPA.

10.3 BMC may disclose Compliance Documentation to: (i) competent Data Protection Authorities acting within the scope of their powers and/or law enforcement authority or agency, or (ii) BMC's clients, only where Company acts as a Sub-Processor of BMC's clients, provided that Compliance Documentation is treated as confidential information, and that the applicable client has entered into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in this DPA.

11. Personal Data Breach Notification to BMC.

11.1 In the event that Company discovers, receives notice of, or suspects a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or

otherwise processed ("**Data Breach**") by Company and its Sub-Processors, Company shall notify BMC without undue delay after becoming aware of the Data Breach at soc@bmc.com, under the conditions of the Incident Management and Breach Notice described in the Information Security Requirements.

11.2 Company shall make reasonable efforts to identify the cause of such breach and take those steps as Company deems necessary and reasonable in order to remediate the cause of such a breach to the extent the remediation is within Company's reasonable control.

11.3 If applicable laws require (i) notice to authorities and/or individuals and/or other entities, (ii) other remedial action; or if BMC determines that notices or other remedial measures are warranted, then, at BMC's request, Company shall undertake such remedial action as BMC may reasonably direct (including, without limitation: improvements or adjustments to Company's information security measures; providing notice to affected individuals, consumer reporting agencies, public authorities, or other entities; providing credit monitoring services; establishing a call center to respond to inquiries).

11.4 BMC shall determine the timing, content and manner of any notice to individuals, consumer reporting agencies or public authorities, and the specific remedial measures to be undertaken. Company shall bear the expense of remedial action to the extent the Data Breach is attributable to the acts or omissions of Company (other than acts or omissions directed by BMC, through its standard operating procedures or otherwise in writing).

12. California Privacy Rights Act. To the extent the CPRA applies to Company's Processing of BMC Personal Data, Company shall: (i) comply with its obligations under the CPRA; (ii) provide the same level of protection as required under the CPRA; (iii) notify BMC if it can no longer meet its obligations under the CPRA; (iv) not "sell" or "share" (as such terms are defined by the CPRA) BMC Personal Data; (v) not retain, use, or disclose BMC Personal Data for any purpose other than to provide the services and/or products to BMC under the Agreement and any applicable ordering document between the parties; (vi) not retain, use, or disclose BMC Personal Data outside of the direct business relationship between BMC and Company; and (vii) not combine BMC Personal Data with Personal Data that Company (a) receives from, or on behalf of, another person or (b) collects from its own, independent consumer interaction, except, in either case, except as permitted under the CPRA. BMC may: (1) take reasonable and appropriate steps to help ensure that Company processes BMC Personal Data in a manner consistent with Company's CPRA obligations; and (b) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing of BMC Personal Data by Company.

13. Personal Data Transfer to Third Countries.

13.1 BMC is committed to complying with its BCR when transferring Personal Data from the country where it was originally collected to another country outside of European Economic Area, Switzerland and or UK as the case may be ("**Third Country**").

13.2 In case of Personal Data Transfers from the European Union to countries not recognized by Data Protection Laws as offering Appropriate Safeguards, the Standard Contractual Clauses, incorporated herein, including their appendices, shall apply completed as follows:

- 13.2.1 Module 2 (Controller-to-Processor) of the Standard Contractual Clauses shall apply where BMC is a Controller and Company is a Processor.
- 13.2.2 Module 3 (Processor-to-Processor) of the Standard Contractual Clauses shall apply where BMC is a Processor and Company is a Processor.
- 13.2.3 in Clause 7, the optional docking clause will apply.
- 13.2.4 The certification of deletion of Personal Data that is described in Clause 8.5 of Modules 2 and 3, as applicable, shall be provided by Company in accordance with Section 9 of the DPA.
- 13.2.5 The audits described in Clause 8.9(c) of Module 2 and Clause 8.9(d) of Module 3, as applicable, shall be in accordance with Section 10 of the DPA.
- 13.2.6 In Clause 17 (Option 1) of Modules 2 and 3, as applicable, the governing law shall be the law of France.
- 13.2.7 In Clause 18(b) of Modules 2 and 3, as applicable, any dispute arising from the EU Standard Contractual Clauses shall be resolved by the courts of France.
- 13.2.8 Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit 1 to the Agreement.
- 13.2.9 Annex II of the EU SCCs shall be deemed completed with the information set out in the Information Security Requirements.

13.3 This DPA and the Agreement are BMC's complete and final documented instructions at the time of signature of the Agreement to Company for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon

separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by BMC to process Personal: (a) Processing in accordance with the Agreement; (b) Processing initiated by BMC in Data its use of the Services; and (c) Processing to comply with other reasonable instructions provided by BMC in writing where such instructions are consistent with the terms of the Agreement. To the extent there is any conflict between this DPA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

13.4 In case of Personal Data Transfers from the UK to countries not recognized as offering Appropriate Safeguards under UK Data Protection Laws, the UK Data Addendum specified in Exhibit 2 shall apply. To the extent there is any conflict between this DPA and the UK Addendum, the terms of the UK Addendum shall prevail.

13.5 BMC and Company acknowledge and agree that in certain circumstances, BMC may be the data Processor and Company shall be a Sub-Processor. In such case and as instructed by BMC from time to time, Company agrees to provide Appropriate Safeguards to BMC's client, including as appropriate Standard Contractual Clauses and/or the UK Addendum.

14. Supplemental Measures.

14.1 Except as BMC directs, Company shall not grant access to Personal Data to any person other than the Sub-Processors, including without limitation a law enforcement authority or agency, or other government entity ("**Requesting Authority**").

14.2 In the event that the Company or any of its Sub-Processor is required by law, court order, warrant, subpoena, and discovery requests or other legal judicial process ("**Request for Disclosure**") to disclose any Personal Data to a Requesting Authority, Company shall provide all reasonable assistance in a timely manner to BMC to enable BMC to respond or object to, or challenge, any such Request for Disclosure and to meet applicable statutory or regulatory deadlines and: (i) put the request on hold and promptly notify BMC in writing upon receiving such Request for Disclosure, unless legally prohibited from doing so by law or by such Requesting Authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Under this section, "promptly" shall be construed as enabling BMC to comply with any applicable Data Protection Laws towards data protection authorities in response to such Requests for Disclosure; (ii) if prohibited from doing so, use its best efforts to inform the Requesting Authority about its obligations under this Agreement and Data Protection Laws, and to obtain the right to waive this prohibition; and (iii) such prohibition cannot be waived, lawfully challenge the Request for Disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflict of laws with applicable Data Protection Laws.

15. Records of Personal Data Processing Activities. Parties shall maintain Records of Processing activities, in their respective roles of Controller and Processor. The Parties shall cooperate to fulfil the obligation to maintain such records. Any material change made by a Party, requiring an update of the Records of Processing activities maintained by the other Party, shall be notified to the other Party within a reasonable time. Each Party shall bear its own costs for its own records of Processing Activities.

16. Cooperation with Competent Supervisory Authorities. Parties shall cooperate with Competent Supervisory Authorities. If a Party is subject to investigative or corrective powers of a Supervisory Authority, this Party shall inform the other Party without undue delay, insofar as it relates to the Services covered by this Agreement. Parties shall provide reasonable assistance to each other to fulfil obligation to cooperate with Supervisory Authorities. Each Party is responsible for its own costs arising from the provision of such assistance.

17. Disclosure of Personal Data.

17.1 Except as BMC directs, Company shall not grant access to Personal Data to any person other than the Sub-Processors, including without limitation a law enforcement authority or agency, or other government entity ("**Requesting Authority**").

17.2 In the event that the Company or any of its Sub-Processor is required by law, court order, warrant, subpoena, and discovery requests or other legal judicial process ("**Request for Disclosure**") to disclose any Personal Data to a Requesting Authority, Company shall provide all reasonable assistance in a timely manner to BMC to enable BMC to respond or object to, or challenge, any such Request for Disclosure and to meet applicable statutory or regulatory deadlines and: (i) put the request on hold and promptly notify BMC in writing upon receiving such Request for Disclosure, unless legally prohibited from doing so by law or by such Requesting Authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Under this section, "promptly" shall be

construed as enabling BMC to comply with any applicable Data Protection Laws towards data protection authorities in response to such Requests for Disclosure; (ii) if prohibited from doing so, use its best efforts to inform the Requesting Authority about its obligations under this Agreement and Data Protection Laws, and to obtain the right to waive this prohibition; and (iii) if such prohibition cannot be waived, lawfully challenge the Request for Disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflict of laws with applicable Data Protection Laws.

18. **Data Protection Training.** Company shall provide adequate data protection awareness training on a periodic basis to its personnel processing Personal Data in the scope of this Agreement.

19. **Remedies.** The Parties acknowledge and agree that the remedy at law for a violation of this DPA may be inadequate and that a breach by Company may cause continuing and irreparable injury to the business of BMC as a direct result of any such violation. The Parties therefore agree that in the event of any actual or threatened violation by Company of this DPA, BMC will be entitled, in addition to any other remedies available to it, to a restraining order and to injunctive relief against the Company to prevent any violations of this DPA, and to any other appropriate equitable or legal relief the court deems proper.

20. **Precedence.** In the event of any conflict or inconsistency between the provisions of this DPA and any of the Agreements executed between the Parties for the subscription and/or purchase of services and/or products by BMC, including prior DPA(s), the provisions of this DPA shall prevail.

EXHIBIT 1 – DATA DESTRUCTION LETTER TEMPLATE

THIS IS A SAMPLE LETTER. PLEASE PREPARE ON YOUR LETTERHEAD IN ACCORDANCE WITH THE DPA.

Date

From:

Company Name

Address

To:

BMC Software, Inc.

2103 CityWest Blvd.

Houston, TX 77042

Attn: Global Procurement

Re: The destruction of BMC Software's personal data

Please be advised that [Company Name] has properly deleted all Personal Data that had been supplied to it under the [Agreement Name] that is dated [date].

Signature

Name of Officer

Title

EXHIBIT 2 - UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers as this term is defined under UK Data Protection Laws. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: BMC (As defined in the Agreement) Trading name (if different): N/A Main address (if a company registered address): As set forth in the Agreement. Official registration number (if any) (company number or similar identifier): As set forth in the Agreement, if applicable.	Full legal name: Company (as defined in the Agreement) Trading name (if different): Specified in Exhibit 1 of the Agreement if applicable. Main address (if a company registered address): As set forth in the Agreement. Official registration number (if any) (company number or similar identifier): As set forth in the Agreement, if applicable.
Key Contact	Full Name (optional): N/A Job Title: Contact details for the Data Exporter are specified in Exhibit 1 of the Agreement. Contact details including email: Contact details for the Data Exporter are specified in Exhibit 1 of the Agreement.	Full Name (optional): Contact details for the Data Importer are specified in Exhibit 1 of the Agreement. Job Title: Contact details for the Data Importer are specified in Exhibit 1 of the Agreement. Contact details including email: Contact details for the Data Importer are specified in Exhibit 1 of the Agreement.
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The Effective Date of the Agreement.

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: "BMC" and "Company" as defined in the Agreement.
Annex 1B: Description of Transfer: As set forth in Exhibit 1 of the Agreement.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth at https://www.bmc.com/documents/various/information-security-requirements.html.
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Exhibit 1 of the Agreement.

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

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

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

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

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
    d. Clause 8.7(i) of Module 1 is replaced with:

       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
    g. References to Regulation (EU) 2018/1725 are removed;

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

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

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

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

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.