



DATA PROCESSING ADDENDUM

This Data Processing Addendum including its Schedules (“**DPA**”) is agreed between Gearset and Customer pursuant to the terms of the [Gearset Master Services Agreement](#) (“**Agreement**”) under which Customer has agreed to procure and Gearset has agreed to provide certain Services (as defined in the Agreement). This is version v1202209 which is effective from 7 October 2022.

This DPA is incorporated into the Agreement by reference, and forms part of the Agreement. It sets out the terms that apply when Gearset Processes Personal Data (as defined in this DPA) on behalf of Customer under the terms of the Agreement. Its purpose is to ensure that such Processing is conducted in accordance with the written instructions of the Customer, as set out in this DPA, and all applicable laws, and with due respect for the rights and freedoms of individuals whose Personal Data are Processed.

NB. This DPA only applies to the extent that Customer uses Gearset’s data migration, masking and/or backup solutions, as that is the only situation in which Gearset Processes Personal Data on behalf Customer.

DATA PROCESSING TERMS:

1 **Definitions**

1.1 Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1.2 For the purposes of this DPA the following words and phrases shall have the following meanings:

"Addendum" means the UK International Transfer Addendum to the EU SCCs, as provided at Schedule 3;

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations;

"Controller" shall mean the entity which, alone or jointly with others, determines the purposes and means of the Processing of the Personal Data;

"Data Protection Laws and Regulations" means all laws and regulations from time to time of the United Kingdom, the European Union and the EEA and their member states, Switzerland, and the United States and its states, applicable to the Processing of Personal Data under this DPA including the UK GDPR; the Data Protection Act 2018 ("**DPA 2018**"); the GDPR; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; the CCPA; and any other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data;

"Data Subject" means the identified or identifiable person to whom Personal Data relates;

"Data Transfer Provisions" means, the EU SCCs and the Addendum;

"EEA" means the European Economic Area, which constitutes the member states of the European Union, Norway, Iceland and Liechtenstein;

"EU SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 2021;

"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, and repealing Directive 95/46/EC (as amended, replaced or superseded);

"Gearset" means Gearset Limited, a company registered in England with company number 10345423 and whose registered office is at The Bradfield Centre, Cambridge Science Park Rd, Cambridge, CB4 0GA, UK;



“**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“**Processor**” shall mean an entity which processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA;

“**Personal Data**” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data (as defined in the Agreement);

“**Security, Privacy and Architecture Documentation**” means the Security, Privacy and Architecture Documentation applicable to the Services purchased by Customer, as updated from time to time, and accessible via Gearset’s security webpage at <https://gearset.com/security> or as otherwise made reasonably available by Gearset;

“**Sub-processor**” means any third party data processor engaged by a Processor who has or will have access to or process Personal Data from a Controller; and

“**UK GDPR**” means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2 Processing of Personal Data

- 2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data as is necessary for providing the Services, Customer may be the Controller or a Processor. Where the Customer is a Controller, Gearset will be a Processor. Where the Customer is itself a Processor, Gearset will be the Customer’s Sub-Processor. In either case, the parties acknowledge and agree that Gearset will engage Sub-processors pursuant to the requirements set forth in clause 5 below.
- 2.2 The Customer acknowledges that Gearset is a controller with regard to the personal data collected by Gearset as part of the sale and/or management of the Subscription (as defined in the Agreement) and/or Services and/or the provision of the Services to Customer, including (but not exclusively) any User Data (as defined in the Agreement). For the avoidance of doubt, this DPA only applies to Customer Data and does not apply to personal data for which Gearset is the controller.
- 2.3 **Customer’s Processing of Personal Data.** Customer: (i) is responsible for ensuring that it has complied, and will continue to comply, with all applicable Data Protection Laws and Regulations; (ii) warrants that it has, and will continue to have, the right to Process, transfer, and/or provide access to, the Personal Data to Gearset for Processing in accordance with the terms of the Agreement and this DPA; and (iii) has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including ensuring that there is a lawful basis for the Processing. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.
- 2.4 **Gearset’s Processing of Personal Data.** Gearset shall Process Personal Data on behalf of Customer as is necessary for providing the Services and only in accordance with Customer’s documented instructions as set out in this DPA. Gearset shall notify the Customer promptly if, in Gearset’s opinion, the Customer’s instructions would not comply with the Data Protection Laws and Regulations. Any Processing required outside of the scope of these instructions will require prior written agreement between the parties. To the extent the CCPA is applicable to Customer’s business and solely with respect to such Personal Data subject to the CCPA, the parties acknowledge and agree that Gearset’s Processing of Personal Data is as a “service provider” as that term is defined under the CCPA for a “business purpose” as that term is defined under the CCPA (i.e., performing services on behalf of Customer).
- 2.5 **Details of the Processing.** The subject-matter of Processing of Personal Data by Gearset, the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data



Subjects Processed under this DPA are further specified in Schedule 1 (Data Processing Appendix) to this DPA.

- 2.6 **Data Protection Impact Assessments.** Upon Customer's request, Gearset shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Gearset. Gearset shall provide reasonable assistance to Customer in the cooperation or prior consultation with the applicable Supervisory Authority in the performance of its tasks relating to clause 2.4 of this DPA, to the extent required under applicable Data Protection Laws and Regulations.

3 Rights of Data Subjects

- 3.1 **Data Subject Request.** Gearset shall, to the extent legally permitted, promptly notify Customer if Gearset receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ('right to be forgotten'), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, solely to the extent each such request is available to the Data Subject under Data Protection Laws and Regulations (each such request being a "**Data Subject Request**"). Taking into account the nature of the Processing, Gearset shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Gearset shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Gearset is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Gearset's provision of any such assistance described in this clause 3.

4 Gearset Personnel

- 4.1 **Confidentiality.** Gearset shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are bound by confidentiality terms no less onerous than those set out in the Agreement. Gearset shall ensure that such confidentiality obligations survive the termination of the personnel engagement for a reasonable period.
- 4.2 **Limitation of Access.** Gearset shall ensure that Gearset's access to Personal Data is limited to those personnel who have a need to access the Personal Data to facilitate the performance of the Services.
- 4.3 **Data Protection Contact.** Gearset has personnel responsible for the protection and Processing of Personal Data. Those personnel may be reached at legal@gearset.com.

5 Sub-processors

- 5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that: (i) Gearset's Affiliates may be retained as Sub-processors, and (ii) Gearset and Gearset's Affiliates may engage third-party Sub-processors in connection with the provision of the Services. Gearset has entered into a written agreement with each Sub-processor containing data protection obligations no less protective than those in this Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- 5.2 **List of Current Sub-processors and Notification of New Sub-processors.** Gearset shall make available to Customer (via the Gearset Website or otherwise) the current list of Sub-processors for the Services ("**Sub-processor List**"). The Sub-processor List shall include the identities of those Sub-processors and their country of location. Gearset shall provide notification of new Sub-processor(s) by updating the Sub-processor List. Gearset shall use reasonable endeavors to alert the Customer of changes to the Sub-processor List through the Software, but the Customer is advised to check the Gearset Website periodically for communications concerning such changes.



5.3 **Objection Right for New Sub-processors.** Customer may object to Gearset's use of a new Sub-processor for a commercially reasonable reason by notifying Gearset promptly in writing within ten (10) business days after Gearset updates the Sub-processor List. In the event Customer reasonably objects to a new Sub-processor, Gearset will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Gearset is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Gearset or Customer may terminate the applicable Subscription(s) with respect to those Services which cannot be provided by Gearset without the use of the objected-to new Sub-processor by providing written notice to the other party. Gearset will refund Customer any prepaid fees covering the remainder of the term of such Subscription(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 **Liability.** Gearset shall be liable for the acts and omissions of its Sub-processors to the same extent Gearset would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6 **Security**

6.1 **Controls for the Protection of Personal Data.** Gearset shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure or access), confidentiality and integrity of Personal Data, as set forth in the Security, Privacy and Architecture Documentation. Gearset regularly monitors compliance with these measures. Customer acknowledges that the security measures are subject to technical progress and development and that Gearset may update or modify the security measures from time to time, provided that such updates and modifications do not result in the material degradation of the overall security of the Services purchased by the Customer.

6.2 **Third-Party Audits.** Gearset engages third party auditors to verify the adequacy of its security measures. These audits (a) will be performed at least annually; (b) will be performed according to internationally recognized standards; (c) will be performed by independent third party security professionals at Gearset's selection and expense and (d) will result in the generation of an audit report ("**Audit Report**") which will constitute Gearset's Confidential Information.

6.3 **Access to Audit Reports.** No more than once during any consecutive 12-month period, on the Customer's written request and subject to the confidentiality obligations in the Agreement, Gearset shall make available to a Customer that is not a competitor of Gearset (or Customer's independent, third-party auditor that is not a competitor of Gearset) a copy of Gearset's then most recent Audit Report or the summary results, as appropriate. Within such request, the Customer shall be entitled to ask reasonable questions of Gearset related to its compliance with the terms of this DPA and Data Protection Laws and Regulations, and Gearset shall use its reasonable endeavors to respond adequately when providing the Audit Report.

6.4 **Sub-processor Audits.** No more than once during any consecutive 12-month period, on the Customer's written request, Gearset will exercise such relevant audit rights that it may have in connection with its Sub-processors' compliance with their obligations regarding their processing of Personal Data, and provide the Customer with a summary of the audit results or, in the event that Gearset has recently exercised such rights for another customer, it shall provide to the Customer a summary of the most recent audit results.

6.5 **Customer's Right to Audit.** Customer agrees to exercise any right it may have to conduct an audit or inspection of Gearset or its Sub-processors by instructing Gearset to carry out the audit described in this clause 6. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Gearset written notice as provided for in the Agreement. If Gearset declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement.

7 **Incident Management and Notification**

7.1 Gearset shall notify Customer promptly and without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored



or otherwise Processed by Gearset or its Sub-processors of which Gearset becomes aware (a “**Personal Data Incident**”).

- 7.2 Gearset shall make reasonable efforts to identify the cause of any Personal Data Incident and take those steps as Gearset deems necessary and reasonable to remediate the cause of such a Personal Data Incident to the extent the remediation is within Gearset’s reasonable control.
- 7.3 The notice to be provided pursuant to clause 7.1 above shall detail, to the extent relevant and reasonably available to Gearset at the time:
- 7.3.1 the date and time of the Personal Data Incident;
 - 7.3.2 the cause of the Personal Data Incident, if known;
 - 7.3.3 the categories and approximate number of records of Personal Data affected;
 - 7.3.4 the likely consequences of the Personal Data Incident;
 - 7.3.5 the measures taken, or proposed to be taken, by Gearset to address and remediate the cause of the Personal Data Incident; and
 - 7.3.6 the name and contact details of the person from whom more information can be obtained.
- 7.4 Gearset shall keep Customer reasonably updated of any material developments to its investigation, handling and remediation of the Personal Data Incident, and Customer and Gearset shall reasonably co-operate to mitigate the risk to each party and the affected data subjects.
- 7.5 The obligations in this clause 7 shall not apply to incidents that are caused by Customer or its Authorised Users, or by access to the Services in breach of clause 4 (Use of Services and Documentation, Customer Obligations) of the Agreement, unless and until the Customer has notified Gearset that they constitute a Personal Data Incident in which case Gearset shall provide the Customer with reasonable assistance (at Customer’s cost) in investigating the information set out in clause 7.3 above.

8 Return and Deletion of Personal Data

- 8.1 Upon termination or expiry of the Agreement, Gearset shall, at Customer's election, delete or return to Customer all relevant Personal Data (including copies) in Gearset’s possession, save to the extent that Gearset is required by any applicable law to retain some or all of the Personal Data.

9 Limitation of Liability

- 9.1 Each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to clause 11 of the Agreement (Limitation of Liability).

10 Transfer Mechanisms

- 10.1 **International Transfers.** It is acknowledged and accepted by Customer that Gearset provides a hosted service which can operate in data centers in various locations around the world, as selected by Customer through the Software. As such, Gearset may transfer Personal Data outside of the UK and EEA as part of its hosting and disaster recovery processes. Customer acknowledges and consents to Gearset transferring Personal Data outside of the UK and EEA for the purposes of providing the Services, provided that any such transfer meets the relevant requirements under the applicable Data Protection Laws and Regulations.
- 10.2 **Data Transfer Provisions.** The Data Transfer Provisions will apply, as applicable, to transfers of Personal Data outside the UK or EEA, whether directly or via onward transfer, where the transfer is: (i) to or within a country not recognized by the UK Government (in the case of transfers made pursuant to the UK GDPR) or European Commission (in the case of transfers made pursuant to the GDPR) as providing an adequate level of protection for personal data; and (ii) no other appropriate safeguard for such transfer as set out in Article 46 of the GDPR is applicable to such transfer. Agreement to this DPA will constitute agreement to the applicable the Data



Transfer Provisions, which shall be incorporated into this DPA by reference. Where the Data Transfer Provisions apply pursuant to this clause 10.2, then in the event of any inconsistency (but not a direct conflict) between the terms of this DPA and the Data Transfer Provisions, the terms of this DPA will prevail. In the event of a direct conflict between the terms of this DPA and the Data Transfer Provisions, the terms of the Data Transfer Provisions will prevail.

11 General Provisions

- 11.1 Except as amended by this DPA, the Agreement will remain in full force and effect.
- 11.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will take precedence.
- 11.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
- 11.4 This DPA will automatically terminate on the termination or expiry of the Agreement.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: EU to Third Country Transfers

Schedule 3: UK International Transfer Addendum to the EU SCCs

SCHEDULE 1 – DATA PROCESSING APPENDIX

1. Data exporter (Controller)

Data exporter is the legal entity specified as Customer in the Agreement/DPA.

2. Data importer (Processor)

Gearset Limited, is a provider of enterprise DevOps software and cloud services.

3. Nature and Purpose of Processing

Gearset will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

4. Duration of Processing

Subject to clause 8 of the DPA, Gearset will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

5. Categories of Data Subjects

Customer may submit Personal Data to Gearset, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

6. Categories of Personal Data

Customer may submit Personal Data to Gearset, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localisation data

7. Sensitive Data (if appropriate)

Customer may submit special categories of data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

8. Frequency of the Transfer

Determined by Customer, in line with its use of the Software.

9. Sub-Processor Transfers

As set out at clause 5 of the DPA.



10. Competent Supervisory Authority

Except where Schedule 2 applies, The UK Information Commissioner
Where Schedule 2 applies, The Irish Data Protection Commissioner.

11. Technical and Organisational Measures

As set out in the Security, Privacy and Architecture Documentation, and accessible at www.gearset.com/security or otherwise made available by Gearset. Gearset will not materially decrease the overall security of the Services during the term of the Agreement.



SCHEDULE 2 – EU TO THIRD COUNTRY TRANSFERS

1. Incorporation of the EU SCCs

1.1. To the extent the transfer is made pursuant to the GDPR, this Schedule 2 and the following terms shall apply:

1.1.1. Module 4 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 2 as if they had been set out in full in the case where the exporter is a Processor, the importer is a Controller and the transfer requires such additional protection.

2. Clarifications to the EU SCCs

2.1. **Module 4 clarifications.** To the extent Module 4 of the EU SCCs applies: (i) paragraphs 1 – 2 of Schedule 1 shall be modified to reflect that the exporter is a Processor and the importer is a Controller; (ii) for the purposes of clause 8.1(d) of the EU SCCs, at the end of the provision of the processing services the importer shall delete all Personal Data and shall certify to the exporter that it has done so, if requested to provide such certification by the exporter in writing; and (iii) for the purposes of clauses 17 and 18 of the EU SCCs, the laws and courts of Ireland shall apply.

3. Appendices and Annexures to the EU SCCs

3.1. The processing details required by the EU SCCs are set out in Schedule 1:

3.1.1. the details required at Annex 1.A of the EU SCCs are set out at paragraphs 1 - 2;

3.1.2. the details required at Annex 1.B of the EU SCCs are set out at paragraph 3 - 9;

3.1.3. the details required at Annex 1.C of the EU SCCs are set out a paragraph 10; and

3.1.4. the details required at Annex 2 of the EU SCCs is set out at paragraph 11.

SCHEDULE 3 – UK INTERNATIONAL TRANSFER ADDENDUM TO THE EU SCCS

Part 1

1. **Parties.** As set out in Schedule 1.

2. Selected SCCs, Modules and Clauses

2.1. Module 4 of the EU SCCs and no other optional clauses unless explicitly specified, and as amended by the clarifications in Schedule 2, paragraph 2, but subject to any further amendments detailed in this Schedule 3 ("**ICO Modified EU SCCs**").

2.2. Personal data received from the importer is not combined with personal data collected by the exporter.

3. Appendix Information

The processing details required by this Addendum are as set out in Schedule 1 ("**Appendix Information**").

4. Termination of the Addendum

In the event the template Addendum issued by the Information Commissioner's Office ("**ICO**") and laid before Parliament in accordance with s119A of the DPA 2018 on 2 February 2022, as it is revised under Section 18 ("**ICO's Addendum**") is amended, either party may terminate this Addendum on written notice to the other in accordance with Part 2, paragraph 4 of this Schedule 3 and replace it with a mutually acceptable alternative.

Part 2

1. Interpretation

1.1. Except as otherwise defined in this Addendum, where this Addendum uses terms that are defined in the EU SCCs, those terms shall have the same meaning as in the EU SCCs.

1.2. This Addendum must always be interpreted:

1.2.1. in a manner that is consistent with 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 (as defined in section 3 of the DPA 2018) and the DPA 2018 ("**UK Data Protection Laws**"); and

1.2.2. so that it fulfils the Parties' obligation to provide the appropriate safeguards, being the standard of protection over the Personal Data and of Data Subjects' rights required by UK Data Protection Laws when a party is making a transfer which is covered by Chapter V of the UK GDPR ("**Restricted Transfer**") relying on standard data protection clauses under Article 46(2)(d) UK GDPR ("**Appropriate Safeguards**").

1.3. If the provisions included in the ICO Modified EU SCCs amend the EU SCCs in any way which is not permitted under the EU SCCs or the ICO's Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the ICO's Addendum will take their place.

1.4. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, the UK Data Protection Laws apply.

1.5. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

1.6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

2. Hierarchy



- 2.1. Although clause 5 of the EU SCCs sets out that the EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in paragraph 2.2 will prevail.
- 2.2. Where there is any inconsistency or conflict between the ICO's Addendum and the ICO Modified EU SCCs (as applicable), the ICO's Addendum overrides the ICO's Modified EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the ICO's Modified EU SCCs provides greater protection for data subjects, in which case those terms will override the ICO's Addendum.
- 2.3. Where this Addendum incorporates EU SCCs which have been entered into to protect transfers subject to the GDPR then the Parties acknowledge that nothing in this Addendum impacts those EU SCCs.

3. Incorporation of and changes to the EU SCCs

- 3.1. This Addendum incorporates the EU SCCs which are amended to the extent necessary so that:
 - 3.1.1. together they operate for data transfers made by the exporter to the importer, to the extent that UK Data Protection Laws apply to the exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - 3.1.2. paragraphs 2.1 to 2.3 override clause 5 (Hierarchy) of the EU SCCs; and
 - 3.1.3. this Addendum (including the 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.
- 3.2. Unless the Parties have agreed alternative amendments which meet the requirements of paragraph 3.1, the provisions of paragraph 3.4 will apply.
- 3.3. No amendments to the EU SCCs other than to meet the requirements of paragraph 3.1 may be made.
- 3.4. The following amendments to the EU SCCs (for the purpose of paragraph 3.1) are made:
 - 3.4.1. References to the "*Clauses*" means this Addendum, incorporating the ICO Modified EU SCCs;
 - 3.4.2. 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*";
 - 3.4.3. 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.*";
 - 3.4.4. 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;
 - 3.4.5. References to Regulation (EU) 2018/1725 are removed;
 - 3.4.6. References to the "*European Union*", "*Union*", "*EU*", "*EU Member State*", "*Member State*" and "*EU or Member State*" are all replaced with the "*UK*" (being the United Kingdom of Great Britain and Northern Ireland);
 - 3.4.7. Clause 13(a) and Part C of Annex I are not used;
 - 3.4.8. The "*competent supervisory authority*" and "*supervisory authority*" are both replaced with the "*Information Commissioner*";
 - 3.4.9. 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;”;

- 3.4.10. Clause 17 is replaced with: “*These Clauses are governed by the laws of England and Wales.*”;
- 3.4.11. 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
- 3.4.12. The footnotes to the EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

4. Amendments to this Addendum

- 4.1. From time to time, the ICO may issue a revised ICO Addendum which:
 - 4.1.1. makes reasonable and proportionate changes to the ICO Addendum, including correcting errors in the ICO Addendum; and/or
 - 4.1.2. reflects changes to UK Data Protection Laws;
- 4.2. The revised ICO Addendum will specify the start date from which the changes to the ICO 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 ICO Addendum from the start date specified in any such replacement ICO Addendum issued.
- 4.3. If the ICO issues a revised ICO Addendum under clause 4.1, if either Party will as a direct result of the changes in the ICO Addendum have a substantial, disproportionate and demonstrable increase in:
 - 4.3.1. its direct costs of performing its obligations under the ICO Addendum; and/or
 - 4.3.2. its risk under the ICO 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 terminate this Addendum on fourteen (14) days' written notice to the other Party before the start date of the revised ICO Addendum.
- 4.4. 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.