HITACHI
Inspire the Next

Data Protection Agreement

1. Introduction

This Data Protection Agreement (the "**DPA**") reflects the Parties' agreement with respect to the Processing of Hitachi's Personal Data by Supplier under the Procurement Agreement including any SOWs thereunder (collectively, the "**Agreement**"). Each Party agrees that it has the ability and full legal authority to perform its obligations under this DPA. For the purposes of this DPA, the obligations of each Party hereunder shall also apply to its respective Affiliates who in Hitachi's case are utilizing the Services and in Suppliers' case providing the Services.

2. Definitions

Unless expressly defined in this DPA, all capitalized terms shall have the same meaning as in the Agreement. In this DPA, the following terms have the following meanings:

Adequate Country: a country or an international organization that the European Commission has determined, by means of an implementing act, ensures an adequate level of protection under Data Protection Laws, including Article 45 of the General Data Protection Regulation.

Data Protection Laws: means any applicable laws relating to the processing of Personal Data

Data Protection Authorities: the relevant statutory authority in each jurisdiction in accordance with Data Protection Laws

Effective Date: the effective date of the Agreement.

Minimum Protection Measures: means the technical and organizational measures specified in the Agreement (Information Security Addendum).

Personal Data: personal information about an identifiable person, which is Processed by Supplier for or on behalf of Hitachi for the Purpose.

Processing: any operation or set of operations which is performed on 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.

Purpose: fulfillment of the Parties' obligations in the Agreement.

Sell: selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal information to a third party for monetary or other valuable consideration.

Standard Contractual Clauses: the standard contractual clauses for data transfers between the European Economic Area and certain non-European Economic Area jurisdictions, promulgated by the EU Commission Decision 2021/914/EU incorporated herein by reference.

Sub-processor: any third party engaged by Supplier or by Supplier's contractor or agent, which Processes Hitachi Personal Data for or on behalf of Supplier for the Purpose.

Term: commences upon the Effective Date and remains in effect continuously until the latest of: (i) the termination or expiration of the Agreement; (ii) such time as Supplier ceases to be authorized by Hitachi to Process Personal Data; or (iii) such time as Supplier (or its Sub-processor) ceases Processing Personal Data.

3. Supplier's Obligations

(a) At all times, Supplier shall treat Personal Data as Confidential Information and shall require all of its Personnel and Sub-processors with access to Personal Data to do the same.

(b) Supplier will remain, at all times, the data controller for any personal data that Supplier provides to Hitachi. Supplier is responsible for compliance with its obligations as the data controller under Data Protection Laws.

(c) At all times, Supplier shall comply with: Data Protection Laws to the full extent applicable to such Personal Data; and the obligations imposed on it in this DPA. To the extent Supplier collects consent(s) for Processing of Personal Data, Supplier shall provide such consent(s) and relevant documentation, as may be reasonably requested by Hitachi, within 72 hours of Hitachi's request.

(d) Supplier shall only Process Personal Data for the Purpose and only in accordance with the written instructions of Hitachi, which include the Agreement and this DPA.

(e) As between the Parties, all Personal Data and derivations thereof, whether or not in deidentified, anonymized, or aggregate form, shall at all times be the property of Hitachi.

(f) Supplier shall ensure that all of its Personnel or Sub-processors performing under this DPA are: (i) required to complete annual data protection training and (ii) subject to contractual terms at least as protective of Personal Data as those in this DPA.

(g) Supplier shall ensure that access to Personal Data is limited to the Personnel or Sub-processor(s) of Supplier who require access for the Purpose. Such access shall be limited in scope to the minimum amount of Personal Data necessary for the Purpose.

(h) Supplier shall implement appropriate technical and organizational measures to protect Personal Data, including against a Security Breach. For the longer of: (i) the Term of this DPA; or (ii) any time period for which Supplier Processes, controls or possesses Personal Data; such measures shall be at least as protective as the Minimum Protection Measures.

(i) Supplier shall not, directly or indirectly: divulge; make public; or otherwise disclose Personal Data to any third party, except after obtaining the express written consent of Hitachi. To the extent permitted by applicable law, Hitachi reserves the right, in its sole discretion, to condition such consent upon Supplier's acceptance of additional terms.

(j) Supplier shall notify Hitachi without undue delay upon Discovery that Supplier or its Sub-processor has failed to comply, or is otherwise unable to comply, with one or more of its obligations under this DPA. In the event of such non-compliance and without limiting any other remedies available to Hitachi under this DPA or applicable law, Hitachi may instruct Supplier to cease Processing Personal Data, and Supplier shall comply with Hitachi's reasonable directions regarding the Personal Data in Supplier's possession or control.

(k) Supplier shall promptly, and in any event within forty-eight (48) hours of Discovery by Supplier, notify Hitachi of any inquiries, investigations, complaints, and claims by third parties (including Data Protection Authorities) that relate to Personal Data. Supplier shall provide reasonable cooperation with Hitachi as necessary for Hitachi to respond to such third parties.

(l) Supplier shall comply with applicable decisions of Data Protection Authorities, arbitrators, or courts relating to the Processing of Personal Data.

(m) To the extent the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §1798.100 et seq. is applicable, Supplier affirms that it shall not: (i) Sell Personal Data; (ii) retain, use, or disclose Personal Data for any purpose, whether commercial or not, other than performing its obligations under the Agreement; or (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Hitachi and Supplier. By executing the Agreement, Supplier certifies that it understands and shall comply with the terms of this Section 3(m).

4. Data Subject Requests

(a) In the event Supplier receives a data subject request related to Personal Data, Supplier shall forward all details related to such request to Hitachi at privacy@hitachivantara.com within forty-eight (48) hours of Supplier's receipt. Supplier shall not respond to data subject requests related to Personal Data.

(b) Unless otherwise agreed in writing by the Parties, Supplier shall, at no additional cost to Hitachi, comply with Hitachi's reasonable requests related to Hitachi's compliance with applicable Data Protection Laws and Hitachi's handling of data subject requests related to Personal Data. This includes, but is not limited to, Supplier's cooperation with Hitachi to address privacy complaints and meet individual data subjects' lawful requests with respect to Personal Data.

5. Sub-Processing

(a) Supplier has Hitachi's general authorization for the engagement of sub-processors. The Supplier shall inform in writing Hitachi of any intended changes concerning the appointment or replacement of sub-processors by submitting a Sub-processor Request, as below in Section 5 b) of this DPA. All Sub-processors approved by Hitachi as of the Effective Date, if any, are expressly listed in the Agreement.

(b) At least 30 days prior to engaging a new sub-processor, Supplier shall submit to Hitachi a "**Sub-processor Request**" describing in detail (i) the intended sub-processor, (ii) the scope of services and obligations to be sub-contracted, (iii) the categories of Personal Data to be Processed by the intended sub-processor, and (iv) the method by which the intended sub-processor would access or receive Personal Data. Supplier shall respond promptly to any request by Hitachi for additional information about the intended sub-processor.

(b) Hitachi may, within 30 days of receiving such Sub-processor Request, notify Supplier of its objection to the new sub-processor. Objection to any new sub-processor is at Hitachi's sole discretion, without need for justification. To the extent Hitachi objects to a new sub-processor, the Parties shall, in good faith, attempt to find a mutually acceptable resolution within 30 days of Hitachi's objection. If Hitachi does not object to the new sub-processor within the 30-day period outlined in this Section, Supplier may deem Hitachi to have no objection to the new sub-processor.

(b) To the extent Supplier engages Sub-processors, it will do so only by way of a written agreement with the Sub-processor on terms which are no less restrictive on the Sub-processor than are imposed on the Supplier under this DPA. At all times, Supplier shall remain fully liable to Hitachi for the performance of the Sub-processor.

(c) Notwithstanding anything else in this DPA, Supplier agrees that it shall not appoint any Sub-processor if Supplier is not satisfied on reasonable grounds that the Sub-processor protects Personal Data with technical and organizational security measures that are at least as protective as the Minimum Protection Measures. Supplier shall take steps to ensure that such technical and organizational security measures are employed by Sub-processor during any Processing of Personal Data.

6. Cross-Border Data Transfer

(a) Supplier shall not transfer any Hitachi Personal Data outside of the European Economic Area, Switzerland or United Kingdom unless: (i) the receiving territory is an Adequate Country; (ii) Supplier has entered into Standard Contractual Clauses sufficient to enable such onward transfer; (iii) the receiving party has sufficient Binding Corporate Rules; or (iv) the receiving party is certified under the EU-US Data Privacy Framework dated 10th July 2023 and maintains such certification continuously throughout the Term.

(b) The Parties agree that the Standard Contractual Clauses are hereby incorporated by reference into this DPA and apply between Hitachi and Supplier, when the transfer of Hitachi Personal Data from Hitachi ("Data Exporter") to Supplier ("Data Importer") is a restricted transfer and

Data Protection Laws require that a valid transfer mechanism be put in place. Hitachi is Data Exporter on its behalf and on behalf of its subsidiaries established within the European Economic Area, the United Kingdom and Switzerland.

(c) Such restricted transfers shall be subject to the Standard Contractual Clauses and these shall be completed as following:
- (i) Modules One, Two and Three will apply (as applicable);
- (ii) In Clause 7, the optional docking clause will apply;
- (iii) Only for Modules Two and Three: In Clause 9, option 2 "General Written Authorization" for Sub-Processors shall apply and the time period for prior notice shall be as set out in Section 5 (b) of this DPA;
- (iv) In Clause 13, the competent supervisory authority shall be the Irish Data Protection Commissioner;
- (v) In Clause 17, the Standard Contractual Clauses shall be governed by Irish law;
- (vi) In Clause 18(b), the parties agree that disputes shall be resolved before the courts of Dublin, Republic of Ireland;
- (vii) Annex I and III of the Standard Contractual Clauses shall be completed with the information set out in Exhibit B of the Agreement; and
- (viii) Annex II of the Standard Contractual Clauses shall be completed with the information set out in Exhibit C of the Agreement.

(d) For the purpose of the DPA, the following applies to data transfers from Switzerland to a third country:
- (i) Competent supervisory authority in Annex I.C under Clause 13 – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)/ Federal Data Protection and Information Commissioner (FDPIC).
- (ii) Applicable law for contractual claims under Clause 17 – Swiss law.
- (iii) Place of jurisdiction for actions between the parties pursuant to Clause 18(b) – Switzerland.
- (iv) Adjustment concerning the place of jurisdiction for actions brought by data subjects – in regard to Clause 18(c) – the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c). For this purpose the Parties agree that Swiss courts are an alternative place of jurisdiction for such data subjects.
- (v) Adjustment regarding references to the GDPR – the references to the GDPR should be understood as references to the Federal Act on Data Protection (FADP) insofar as the data transfers are subject to the FADP.

(e) For the purpose of the DPA, Schedule 1 to this DPA applies to transfer of Hitachi Personal Data from Hitachi to Supplier is a restricted transfer from United Kingdom to a third country.

7. Termination

(a) Supplier shall, at Hitachi's reasonable election, promptly return or destroy Personal Data Processed on behalf of Hitachi at the end of the Term. If Hitachi requests that Supplier destroy Personal Data, Supplier shall, within thirty (30) days of Hitachi's request, certify in writing that it (i) destroyed the Personal Data so as to render the data unreadable and (ii) confirmed that any Sub-processors have done the same.

(b) Unless otherwise agreed in writing by the Parties, such return or destruction shall be completed within ten (10) days after the end of the Term.

8. Miscellaneous

(a) The invalidity or unenforceability of any part of this DPA for any reason whatsoever will not affect the validity or enforceability of the remainder.

(b) Except as permitted by Section 5 of this DPA, Supplier shall not transfer its obligations under this DPA without Hitachi's prior written consent.

(c) This DPA, together with the Agreement, constitutes the entire agreement and understanding between the Parties with respect to its subject matter and replaces all previous agreements between, or understandings by, the Parties with respect to such subject matter. In the event of any conflict or inconsistency between the terms of this DPA and those of the Agreement, the terms of this DPA will be controlling to the extent of the conflict. This DPA may not be modified except in writing executed by both Parties.

(d) This DPA is entered into for the benefit of the individuals whose Personal Data is Processed by Supplier and any such individual is hereby entitled to enforce this DPA as a third-party beneficiary.

HITACHI
Inspire the Next

Schedule 1 to the DPA

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	With the Effective Date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	**Name**: Hitachi Affiliates based in the United Kingdom. **Address**: Sefton Park, Bells Hill, Stoke Poges, Buckinghamshire, SL2 4HD, United Kingdom	**Name**: Supplier as outlined in the Agreement **Address:** Supplier as outlined in the Agreement
Key Contact	**Contact person's name, position and contact details for operational matters**: Ben Jones - Global Privacy Counsel - privacy@hitachivantara.com **For data protection matters:** 2535 Augustine Drive, Santa Clara, CA 95054 U.S.A privacy@hitachivantara.com	**Contact person's name, position and contact details**: As outlined in the Agreement

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:** With the Effective Date of the Agreement **Reference (if any): N/A** **Other identifier (if any): N/A** **Or** **the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:**

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1		**X**		n/a	n/a	Yes, only if required to fulfil the purpose.
2, 3		**X**		General Authorisation	At least 30 days	Yes, only if required to fulfil the purpose.

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 described in the DPA and the Agreement.

Annex 1B: Description of Transfer: As described in Exhibit B to the Agreement.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Exhibit C to the Agreement.

Annex III: List of Sub processors (Modules 2 and Three): As described in Exhibit B to the Agreement.

HITACHI
Inspire the Next

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 20.** If the ICO issues a revised Approved Addendum under Section 18. From time to time, the ICO may issue a revised Approved Addendum which:, 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:**:** **Importer** **Exporter**

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 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. From time to time, the ICO may issue a revised Approved Addendum which:.
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. 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. 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 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. 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. will prevail. to 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. 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. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:, the provisions of Section
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:) are made: will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that: may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:) 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.";
    (a) 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";

(b) 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;"

(c) 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".

(d) References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(e) References to Regulation (EU) 2018/1725 are removed;

(f) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

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

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

(i) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(j) 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;";

(k) Clause 17 is replaced with:
"These Clauses are governed by the laws of England and Wales.";

(l) 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

(m) 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;
19. 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.
20. If the ICO issues a revised Approved Addendum under Section
18. From time to time, the ICO may issue a revised Approved Addendum which:, 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.
21. 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.