DATA PROTECTION AGREEMENT TEMPLATE – EU SCC’S/UK ADDENDUM

	Party 1	Party 2
Company name		
Data protection position	Controller	Controller
Does this include affiliates of the party, pursuant to the Agreement? (Yes/No)?		
Address		
Company number (if applicable)		
Effective date of the Data Protection Agreement		

Duly signed, for and on behalf of:

	Party 1		Party 2
By (signature):	________________________	By (signature):	________________________
Name:	________________________	Name:	________________________
Title:	________________________	Title:	________________________
Date:	________________________	Date:	________________________

DATA PROTECTION AGREEMENT

This Data Protection Agreement (the "**Agreement**") is entered into by the parties identified on page 1 of the Agreement (each a "**Party**" and together the "**Parties**") and is effective as of the date identified on page 1 of the Agreement (the "**Effective Date**").

BACKGROUND

A. [Party 1] and [Party 2] are parties to one or more Terms of Business Agreements, by means of which the Broker is granted authority to act as agent to arrange insurance on with one or more Underwriting Members of Lloyd's, including [ ] (the "Terms of Business Agreements").

B. In the performance of its obligations and activities under the Terms of Business Agreements, each Party independently determines the purposes and means of processing, and as such, acts as a Controller of any Personal Data.

C. The Parties wish to regulate their mutual obligations regarding compliance with Data Protection Law in regard to International Data Transfers.

IT IS HEREBY AGREED AS FOLLOWS

1. PURPOSE

In consideration of the payment by each Party of £1 (one pound sterling) to the other, receipt of which is hereby acknowledged and deemed accepted, the Parties agree to this Agreement, which sets out the framework for the IDTs conducted by the Parties in the performance of their obligations under the Terms of Business Agreements. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

2. COUNTERPARTS

The Agreement may be executed in any number of counterparts, and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart.

Each counterpart shall constitute an original of the Agreement, but all the counterparts shall together constitute one and the same instrument.

3. GOVERNING LAW

The Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the provisions of the Terms of Business Agreements.

4. THIRD PARTIES

The Agreement is only meant to regulate the Parties' mutual obligations. Nothing in the Agreement, express or implied, is intended to or shall confer upon any person who is not a party to the Agreement any right, benefit or remedy of any nature whatsoever under or by reason of the Agreement.

5. STANDARD CONTRACTUAL CLAUSES

5.1. From the Effective Date, in the performance of the Parties' obligations under any existing or future Terms of Business Agreements, the Parties will comply with this Agreement, the Standard Contractual Clauses ("SCCs") and the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum"), all of which are enclosed to this Agreement as Exhibit 1.

5.2. The Parties agree that:

a. Where in the performance of a Terms of Business Agreement there is an International Data Transfer subject to EU Data Protection Law, the Parties shall comply with the terms of the EU Standard Contractual Clauses and their Annexes I and II;

b. Where in the performance of a Terms of Business Agreement there is an International Data Transfer subject to UK Data Protection Law, the Parties shall comply with the terms of the EU Standard Contractual Clauses, their Annexes I and II, and the UK Addendum;

c. In the cases of Sub-sections 5.2 (a) and (b) above, the provisions of Exhibit 1 shall be construed and applied jointly with other provisions in the respective Terms of Business Agreement which regulate the same matters; however, where there is any inconsistency or contradiction between the provisions of Exhibit 1 and the other provisions, the provisions Exhibit 1 will prevail; and

d. Annexes I, II, and III and the UK Addendum (if applicable) should be populated with the relevant information on the International Data Transfer.

6. DEFINITIONS

6.1. The terms defined in the Terms of Business Agreements, including Controller, Processor and Personal Data, shall have the meanings set forth therein.

6.2. Additionally, for the purposes of the Agreement:

*(a) "**International Data Transfer**" (or "**IDT**") means Transfer of Personal Data from the EU/UK to a Third Country;*
*(b) "**Third country**" means a country that is not part of the EEA/UK (as applicable) and has not been found to have adequate levels of protection to Personal Data[1].*

7. EFFECTIVE DATE

The Parties acknowledge and agree that in the event that the Broker does not sign and date this Addendum by [ ], then the Broker's continued activities under the Terms of Business Agreements on or after that date shall be deemed agreement by the Broker to the provisions of the Agreement as if the Broker had signed the Agreement.

8. TERM

The Agreement shall commence on the Effective Date and remain in force until all the Terms

[1] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

of Business Agreements between the Parties have terminated.

EXHIBIT 1
Controller to Controller EU Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([2]) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 12 – Module One: Clause 12(a) and (d

(iv) Clause 13;

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

(vi) Clause 16(e);

(vii) Clause 18 – Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (3) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data

[3] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union [4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

Not applicable to Controller to controller agreements.

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[5] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients

[5] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter ‘automated decision’), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III

LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (6);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(f) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(g) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(h) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(a) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(b) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: [ ]

   Address: [ ]

   Contact person's name, position and contact details: [ ]

Activities relevant to the data transferred under these Clauses: negotiation, execution and management performance of the insurance contract and performance of the parties' activities under the insurance contracts.

Signature and date: ____

Role (controller/processor): Controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: ___________________________

   Address: ___________________________

   Contact person's name, position and contact details: ___________________________

   ____

   ____

Activities relevant to the data transferred under these Clauses: negotiation, execution and management performance of the insurance contract and performance of the parties' activities under the insurance contracts.

Signature and date: ____

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Policyholders and insured persons
- Brokers
- Third Party administrators
- Other insurers/reinsurers
- Employees of insurers/reinsurers

Categories of personal data transferred

- Contact details
- Policy information
- Claim information
- Financial information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Health Information
- Criminal history

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

- Continuous or as required for the performance of the insurance contract

Nature of the processing

- Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data as required for the negotiation, execution and management of the insurance contracts and performance of the parties' activities.

Purpose(s) of the data transfer and further processing

- Marketing and sales of insurance
- Performance of the insurance contract
- Maintaining accurate records of all claims

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

- Information will be retained in accordance with the Parties' data retention policies and schedules.

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

- N/A

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commissioner (DPC)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. SYSTEMS CONTROL:

A. Measures for pseudonymisation and encryption of person data, both in transit and at rest.

B. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

C. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational security measures in order to ensure the confidentiality, integrity and availability of the data and systems.

D. Measures for ensuring secure system configuration, including changes to default configuration to uplift security.

E. Patch management on minimum monthly basis must be performed to prevent malicious code and out of band patching must be available for zero-day events.

F. Email gateway filtering, intrusion prevention systems, antivirus, 24*7*365 security log monitoring, data loss prevention systems and firewall controls must be implemented in the infrastructure.

G. Procedures to ensure that focus must given to security issues during application design and development (SDLC process).

H. Procedure to guarantee thorough security testing and secure packaging of software prior to its release into the production environment.

2. POLICY CONTROL:

A. Data importer must maintain an information security policy that, at a minimum, includes:

i. a definition of information security, its overall objectives and scope and the importance of security to data importer;

ii. a statement of management intent;

iii. a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

iv. a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including, without limitation, compliance with legislative, regulatory, and contractual requirements, security education, training, and awareness requirements, business continuity management and consequences of information security policy violations);

v. a definition of general and specific responsibilities for information security management, including, without limitation, reporting information security incidents; and

vi. references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules with which users must comply.

B. On reasonable request of [ ], Service Provider shall cooperate in the conduct of any Information Security assessments such as security architecture assessment, Penetration testing, threat risk assessment on the solution, however that any information obtained by [ ] in connection with or in the course of any such assessment and any such information provided to or obtained by [ ] shall be maintained by [ ] in the strictest confidence, shall be used solely for the purposes of ensuring that Service Provider is complying with [ ] information security standards.

C. Data importer shall ensure that its information security policy covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and other devices and media that process or handle any Information Assets as they relate to this agreement.

D. Policy measures for internal IT and IT security governance and management include:

i. IT security policies for the secure operation, management and development of system and handling of data;
ii. IT General User policy;
iii. Information Classification
iv. Record Retention Program;
v. Incident management standards and process;
vi. Business Continuity Program;
vii. BYOD (Bring Your Own Device) Policy;
viii. Internal Security audit program
ix. Mobile Device Security Standards, incorporating laptop, mobile and handheld device encryption
x. Enterprise Vulnerability Management Program, conducting routine vulnerability scans and timely remediations of identified vulnerabilities.
xi. Enterprise Data Loss Prevention Program

3. SECURITY INCIDENT CONTROL:

A. If a disclosure, outbreak, violation or other breach of data importer security standards in this Annex occurs, data importer will promptly take all steps necessary to prevent any further damage to/exposure of any information, unauthorized use, duplication, or modification of information assets as they relate to this arrangement.

B. Data importer will notify data exporter within 24 hours of identifying an incident and provide updates on a consistent and reasonable timeframe.

C. Importer should cooperate in order to identify and investigate the root cause of the incident. It should also seek to prevent unauthorized use, duplication, or modification of the information. These processes should be supported by procedures for identification, reporting, assessment, response, recovery and review. Procedures containing a clear allocation of roles and responsibilities within all teams involved in the incident investigation and risk mitigation activities should be put in place.

D. Importer should set up IT systems, applications and network devices to generate and record security event logs in order to assist in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations. Importer must ensure that all the logs generated by IT systems, applications and network devices are stored, retained and protected from unauthorized access, destruction and modification in accordance with business requirements.

4. EMPLOYEE CONTROL:

A. Security awareness and training for all employees with refresher training and updates.

B. All employees be subject to stringent screening prior to employment using a third-party provider. The screening processes will be conducted in accordance with relevant national laws and industry regulations and provide verification of identity and credentials and will include an evaluation ok applicant integrity through a comprehensive reference checking process. Temporary employees shall be evaluated in substantially the same manner as permanent employees and importer shall audit contract staffing agencies to ensure compliance with the screening processes through the regional third-party supplier management programs.

5. THIRD PARTY CONTROL:

A. Measures relating to third party control management. Measures include:
   i. Perform Security Due diligence;
   ii. Documented approvals;
   iii. Security and incident handling Contract terms;
   iv. SLAs; NDAs and
   v. Maintaining minimum security standards as per importers policies.

B. Measures relating to Cloud Service Security Standards

C. Measures for security certification/assurance of processes and products.

D. Third party access or sharing of [ ] data with any third party must be approved by [ ] officials.

E. Periodic assessment of the information security status of suppliers assigned a rating of critical or high, at a frequency that is commensurate with that criticality rating.

6. PHYSICAL ACCESS CONTROL:

A. Measures for ensuring physical security of locations at which personal data are processed. Measures include:
   i. Access to entry doors and sensitive areas;
   ii. Securing and limiting access to server rooms;
   iii. Installing video cameras where appropriate;
   iv. Using electronic ID badges, access swipe cards for entering data importer’s offices;
   v. Controlling badge holder access and logging; and
   vi. Alarm monitoring.

7. AVAILABILITY CONTROL:

A. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

B. Technical measures to ensure that personal data stored in data importer’s internal systems are protected against accidental destruction or loss. Measures include:
   i. The use of protection programs (such as firewall, SPAM filters, IDS/IPS, DLP);
   ii. Single sign on (SSO) or MFA authentication mechanisms must be used for authentication;
   iii. Rejection of unauthorized users; and
   iv. Backup, recovery and restoration measures.

8. TRANSFER CONTROL:

A. Technical measures to prevent personal data from being processed or used during electronic transmission or during transport without authorization (e.g. by means of encryption or protection by certificates). Measures include:

i. Authentication of authorized personnel (Single sign on (SSO) or MFA authentication mechanisms used for authentication);
ii. User identification measures; and
iii. Controlling the removal and destruction of data media.

9. LOGISTICAL ACCESS CONTROL:

A. Measures to prevent data processing systems from being used without authorization. Measures include:
i. Locking of terminals;
ii. Regulations for user authorization;
iii. Setting user (re)certifications, privileges, access rights;
iv. End user workstation access controls including password minimum requirements and controls, SSO;
v. Obligation to comply with data confidentiality requirements;
vi. Differentiated access regulations (e. g. partial blocking);
vii. Controlled destruction of data media;
viii. Network/infrastructure, application and database access controls – job function "need to know" and least privilege requirements;
ix. Remote/external access control; token enabling two factor authentication; and
x. Single sign on (SSO) or MFA authentication mechanisms used for authentication.

10. INTERVENTION CONTROL:

A. Measures to implement data processing systems from being used by unauthorized persons by means of data transmission equipment. Measures include:
i. Access and authorization concepts; and
ii. Different user ID´s and passwords for access to data processing systems.

11. SUPPLEMENTARY MEASURES (US SPECIFIC)

In addition to the measures set out above:

1. Written Records
1.1. The Data Importer will keep detailed, accurate and up-to-date written records (the **Records**) regarding requests for and/or access to the data by state or public entities including enforcement bodies. The log must contain at least the following information:
1.1.1. date request received by the Data Importer;
1.1.2. date the Data Importer notified the Data Exporter of the request;
1.1.3. date of access to the data by the state/public entity;
1.1.4. individuals and personal data concerned;
1.1.5. the accessing enforcement body; and
1.1.6. the basis invoked by the enforcement body to justify access to the information.

1.2. The Data Importer will ensure that the Records are sufficient to enable the Data Exporter to verify the Data Importer's compliance with its obligations under this Agreement.

1.3. The Data Importer will provide the Data Exporter at the end of each month with copies of the Records.

1.4. Further copies of the Records will be provided to the Data Exporter by the Data Importer upon request.

2. Requests for access by third parties

2.1. Before the Data Importer discloses any personal data pursuant to a request for and/or access to the data by a third party, including state or public entities and enforcement bodies, it shall notify the other party a soon as possible and, in any case, no later than 24 hours after the Data Importer has received the request.

2.1.1. The Data Importer shall take into account the Data Exporter's requests in relation to the content of any such disclosure.

2.1.2. In the event that the Data Exporter objects to the disclosure, the Data Importer will use all reasonable endeavours to support the Data Exporter to prevent or limit the disclosure.

2.2. If the Data Importer is prohibited from informing the Data Exporter before personal data is disclosed pursuant to a request for and/or access to the data by a third party, including state or public entities and enforcement bodies, it shall, to the extent permitted by law, inform the Data Exporter of the full circumstances of the disclosure and the information that has been disclosed as soon as reasonably practicable after such disclosure has been made.

12. ADDITIONAL CONTRACTUAL MEASURES

(1) Complement to Clause 8.9 (c)

The Parties agree to add at the end of Clause 8.9 (c):
"For avoidance of doubt, any personal data disclosure or access from public authorities may, at the data exporter's option, be subject to an audit, for the purpose of verifying such access or disclosure did not exceed what is necessary and proportionate in a democratic society. "

(2) Complement to Clause 14

The Parties agree to add at the beginning of Clause 14 (a) the following:
"(a) In order to allow the data exporter to achieve its obligations under Clauses 8 and 14, the data importer warrants it has completed the "transfer questionnaire" (hereinafter "Questionnaire"), to the best of its knowledge and with its best efforts in order to assist the Data Exporter in assessing the impact of the transfer.

The Parties agree to add at the end of Clause 14 (e) the following:
"In the event of such notification, and in accordance with Clause 14 (c), the data importer shall assist without any delay the data exporter to the best of its knowledge and with its best efforts to update the Questionnaire and re-assess the transfer impact assessment to ensure the compliance of the transfer with its own obligations."

The Parties agree to modify Clause 14 (f) as follows:
"(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be

adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if the data importer failed to implement appropriate measures identified by the data exporter without undue delay following the communication of these measures to the data importer or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, as of right and without the need of any judicial formality, simply by sending a written notice by registered letter with acknowledgement of receipt. The Customer shall only be liable to pay the sums applicable for the Services up to the effective termination date and any prepaid fees shall be reimbursed for the portion terminated. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply."

(3) Complement to Clause 15

The Parties agree to add the following in Clause 15.1 (a):
"(a) The data importer agrees to notify as soon as it receives and in any case no later than one (1) business day the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (…)
And add at the end of such Clause 15.1 (a):
"(…) The notification must take place prior to any access or disclosure is granted in order to prevent potential violation of applicable laws and regulations and to allow the data exporter to take appropriate measures to fulfil its duty, including suspending the transfer, retrieving the personal data to the third country and/or terminate the Agreement. In the event of such notification, the data exporter may, at its option, ask the data importer to notify simultaneously the competent supervisory authority from the EEA as indicated in Annex I.C, insofar as possible under the third country legal order of such request or order."

The Parties agree to add the following at the end of section 15.1 (b):
"The notification shall take place as soon as the prohibition is lifted or lapses."

The Parties agree to add a new Clause 15.1 (f):
"(f) To the extent legally admissible, where the data subject is notified of the request, the data exporter may request that the concerned data subjects be informed of the data importer's inability to comply with the contractual commitments the data exporter has towards the data importer, in order to enable the data subjects to seek information and/or effective redress (e.g., by lodging a claim with his/her competent supervisory authority and/or judicial authority and demonstrate his/her standing in the courts of the transfer country.).
In the event such information is not legally possible prior to disclosure, the data importer shall challenge, on a best effort basis, the prohibition to disclose in accordance with Clause 15.2, and shall inform the data subject as soon as such restriction is lifted.
Upon request from the data exporter and/or the data subject, the data importer shall give the data subject reasonable assistance in order to inform him/her of the applicable laws and regulations in the third country as well as challenging the order or the request."

The Parties agree to add the following at the end of the first sentence of Clause 15.2 (a):

“The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity or where the data exporter (when notified by the data importer of such request) decides the legality of such request should be reviewed. (…) When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. The data importer shall also inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 of General Data Protection Regulation transfer tool and the resulting conflict of obligations for the data importer. (…);”.

(4) Supplementary measure on applicable laws and regulations in the destination country

The data importer warrants to the data exporter that:

applicable laws and regulations or governmental policies applicable to the data importer or in the transfer country do not require that the data importer:

a. creates or maintains back-door or facilitate access to its information systems and/or to the personal data;

b. be in possession and/or to hand over to the public authorities the encryption key.

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

(“UK Addendum”)

Table 1: Parties and Signatures

Start Date:	This IDTA is effective as of the Effective Date	
The Parties	**Exporter (Who Sends the Restricted Transfer)**	**Importer (Who Receives the Restricted Transfer)**
Parties' Details	**Full legal name**: [INSERT] **Trading name (if different)**: **Main address (if a company registered address)**: : [INSERT **Official registration number (if any) (company number or similar identifier)**: : [INSERT	**Full legal name**: [INSERT] **Trading name (if different)**: **Main address (if a company registered address)**: [INSERT] **Official registration number (if any) (company number or similar identifier)**:
Key Contact	**Full Name**: : [INSERT **Job Title**: [INSERT **Contact Details Including E-Mail**: : [INSERT	**Name**: : [INSERT **Job Title**: : [INSERT **Contact Details Including E-Mail**: : [INSERT
Signature (if required for the purposes of Section 2)	**Name:** ______________________ **Title:** ______________________ **Company:** : [INSERT	**Name:** ______________________ **Title:** ______________________ **Company:** : [INSERT

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**: **Reference (if any)**: **Other identifier (if any)**: **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:

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set forth in Annex 1 to EU Standard Contractual Clauses

Annex 1B: Description of the transfer: As set forth in Annex 1 to EU Standard Contractual Clauses

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex 2 to EU Standard Contractual Clauses

Annex III: List of Sub processors (Module 2): As set forth in Annex 3 to EU Standard Contractual Clauses

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

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.