These Terms and Conditions govern the provision of certain services and the relationship between:

(1) Compliance Assist Limited a company incorporated and registered in England and Wales with company number 6853249 whose registered office is at The Sussex Innovation Centre, Science Park Square, Falmer (**Supplier**); and

(2) The company or entity subscribing for the services whose details are set out on the relevant Service Contract to which these terms and conditions apply (**Customer**)

BACKGROUND

(A) The Supplier is in the business of providing certain services via its proprietary online platform and data matching engine to facilitate Anti-Money Laundering Checks, Sanctions and PEP Screening, Identity Verification and Corporate Risk Screening ("the Services").

(B) The Customer wishes to obtain and the Supplier wishes to provide the Services on the terms set out in this Agreement and the applicable Service Contract containing the variables of the particular Service provision in relation to the Agreement.

(C) Each and every Service Contract will incorporate the terms and conditions set out in this Agreement.

Agreed terms

1. Interpretation

1.1 The following definitions and rules of interpretation apply in this Agreement:

Affiliate: in relation to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party from time to time.

Applicable Data Protection Laws: means:

a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject, which relates to the protection of personal data.

Applicable Laws: all applicable laws, statutes, regulation and codes from time to time in force.

Authorised Users: those employees, agents and independent contractors of the Customer who are authorised by the Customer to use the Services and the Deliverables, as further described in the Service Contract.

Business Day: a day, other than a Saturday, Sunday or public holiday in England, when banks in London are open for business.

Charges: the charges set out in the applicable Service Contract payable by the Customer for the supply of the Services by the Supplier.

Compliance Assist Platform: the proprietary software based online platform and Data Matching Engine incorporating the Software providing access to data held by certain regulators and the databases of relevant third-party commercial entities that has been developed and is managed, maintained and supported by the Supplier to help Customers meet their own customer screening requirements.

Control: the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the general management of the company, and **controls**, **controlled** and the expression **change of control** shall be construed accordingly.

Customer Data: the data inputted by the Customer, Authorised Users, or the Supplier on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services.

Customer Manager: in respect of each Service Contract, the person so designated in the Service Contract.

Customer Materials: all documents, information, items and materials in any form which are provided by the Customer to the Supplier in connection with the Service Contract (if any).

Customer Personal Data: any personal data which the Supplier processes in connection with this Agreement, in the capacity of a processor on behalf of the Customer.

Data Matching Engine: the Supplier's proprietary data matching engine forming an integral part of the Compliance Assist Platform which has been developed to provide Supplier with the ability to match customer data against various data sets.

Data Processing Agreement: the Data Processing Agreement set out in Schedule 2 of the Agreement.

Deliverables: any output of the Services to be provided by the Supplier or its agents, contractors or employees to the Customer as specified in a Service Contract and any other documents, reports, products and materials provided by the Supplier to the Customer in relation to the Services.

EU GDPR: means the General Data Protection Regulation (*(EU) 2016/679*), as it has effect in EU law.

EUA (End User Agreement): any End User Agreement applicable to a Service Contract from time to time.

Initial Subscription Term: the initial term of the Services provision as set out in the relevant Service Contract**.**

Intellectual Property Rights: patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trade marks and service marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

Renewal Period: the period described in the relevant Service Contract (if any).

Services: the services, including without limitation any Deliverables, to be provided by the Supplier pursuant to the relevant Service Contract.

Service Contract: the contract for the provision of certain Services, agreed in accordance with clause 3, relating to the particular Services to be provided by the Supplier.

Supplier Personal Data: any personal data that the Supplier processes in connection with this Agreement, in the capacity of a controller.

Software: the online software applications provided by the Supplier as part of the Services comprised in the Compliance Assist Platform and the Data Matching Engine.

Subscription Fees: the subscription fees payable by the Customer to the Supplier for the User Subscriptions, as set out in the applicable Service Contract.

Subscription Term: the Initial Subscription Term together with any subsequent Renewal Periods specified in the Service Contract or agreed between the Supplier and the Customer.

User Subscriptions: the user subscriptions purchased by the Customer pursuant to the applicable Service Contract which entitle Authorised Users to access and use the Services and the Deliverables in accordance with this Agreement.

Virus: any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service the Compliance Assist Platform, Data Matching Engine or the Software.

Vulnerability: a weakness in the computational logic (for example, code) found in software and hardware components that when exploited, results in a negative impact to the confidentiality, integrity, or availability, and the term **Vulnerabilities** shall be interpreted accordingly.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

VAT: value added tax or any equivalent tax chargeable in the UK or elsewhere.

1.2 All defined terms used in this Agreement and the Service Contract shall have the meaning given to them in this clause 1.

1.3 The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this Agreement includes the Schedules.

1.4 A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5 This Agreement shall be binding on, and enure to the benefit of, the parties to this Agreement and their respective personal representatives, successors and permitted assigns, and references to any party shall include that party's personal representatives, successors and permitted assigns.

1.6 Unless expressly provided otherwise in this Agreement or the relevant Service Contract, a reference to legislation or a legislative provision is a reference to it as amended, extended or re-enacted from time to time.

1.7 A reference to **writing** or **written** includes email.

1.8 Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

1.9 Any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

2. Commencement and duration

2.1 This Agreement shall commence on the dates specified in the Service Contract and shall continue for the applicable Subscription Term unless terminated earlier in accordance with clause 11 (Termination).

2.2 The Customer may procure any of the Services by agreeing a Service Contract with the Supplier pursuant to clause 3 which such Service Contract shall include a Subscription Term.

3. Service Contract Process

3.1 Service Contracts shall be entered into in accordance with this Agreement in the following manner:

(a) the Customer shall ask the Supplier to provide any or all of the Services and provide the Supplier with as much information as the Supplier reasonably requests in order to prepare the applicable Service Contract for the Services requested;

(b) following receipt of the information requested from the Customer the Supplier shall, as soon as reasonably practicable either:

(i) inform the Customer that it declines to provide the requested Services; or

(ii) provide the Customer with a Service Contract for approval.

(c) Upon acceptance of the Service Contract both parties shall enter into the Agreement by signing the Service Contract incorporating its terms together with these Terms and Conditions of Service ("the Agreement").

(d) In the event of a conflict between the terms of this Agreement and any special terms or conditions stipulated in a Service Contract, the terms of the Service Contract will prevail.

3.2 The Subscription Fees and the Charges will be specified in and paid in accordance with the Service Contract and clause 7 of this Agreement.

3.3 Once a Service Contract has been entered into no amendment shall be made to it except in accordance with clause 15 (Variation).

3.4 Each Service Contract shall be part of this Agreement and shall not form a separate contract to it.

4. Supplier's responsibilities and access to the Compliance Assist Platform

4.1 The Supplier shall, during the Subscription Term, provide access to the Compliance Assist Platform and to the Services and make available the Deliverables specified in the relevant Service Contract to the Customer on and subject to the terms of this Agreement.

4.2 The Supplier shall use commercially reasonable endeavours to make the Compliance Assist Platform and the Services available 24 hours a day, seven days a week, except for:

(a) planned maintenance carried out during the maintenance window of 10.00 pm to 2.00 am UK time; and

(b) unscheduled maintenance performed outside Normal Business Hours, provided that the Supplier has used reasonable endeavours to give the Customer notice in advance.

4.3 The Supplier undertakes to use all reasonable expertise, skill and care so as to ensure that the Compliance Assist Platform operates in accordance with its specification and that the Services can be accessed in accordance with the relevant Service Contract.

4.4 The undertaking at clause 4.3 shall not apply to the extent of any non-conformance which is caused by use of the Services contrary to the Supplier's instructions, or modification or alteration of the Services by any party other than the Supplier or the Supplier's duly authorised contractors or agents. If the Services do not conform with the foregoing undertaking, Supplier will, at its expense, use all reasonable commercial endeavours to correct any such non-conformance promptly, or provide the Customer with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of the undertaking set out in clause 4.3.

4.5 The Supplier:

(a) does not warrant that:

(i) the Customer's use of the Services will be uninterrupted or error-free; or

(ii) that the Services, Deliverables and/or the information obtained by the Customer through the Services will meet the Customer's requirements or that the data obtained through the use of third-party feeds will always be accurate or error-free; or

(iii) the Software or the Services will be free from Vulnerabilities or Viruses.

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services and Deliverables may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

(c) is not responsible for the content of, Virus or Vulnerability-free operation or proper functioning of third-party services accessed via an EUA.

4.6 This Agreement shall not prevent the Supplier from entering into similar agreements with third parties, or from independently developing, using, selling or licensing the Compliance Assist Platform, the Software and/or services which are similar to those provided under this Agreement.

4.7 The Supplier warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Agreement.

4.8 The Supplier shall use reasonable endeavours to provide the Services, and deliver the Deliverables to the Customer, in accordance with a Service Contract in all material respects.

5. Customer's obligations

5.1 The Customer shall:

(a) co-operate with the Supplier in all matters relating to the Services;

(b) warrant that the specifications it provides to the Supplier in relation to the provision of the Services are complete and accurate, and comply with all Applicable Laws;

(c) warrant that it will, and ensure that any of its end users will, comply with the EUA and any other third party terms as advised by the Supplier from time to time;

(d) ensure that the maximum number of Authorised Users that it authorises to access and use the Services shall not exceed the number of User Subscriptions that it has purchased under a Service Contract from time to time;

(e) not allow any Authorised Subscription to be used by anyone other than the Authorised User unless it has been reassigned in its entirety to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access to use the Services;

(f) ensure that each Authorised User shall keep its password for their use of the Services confidential and secure;

(g) co-operate with the Supplier in all matters relating to the Services and appoint (and, as it thinks fit, replace) the Customer's Manager in relation to the Service Contract; and

(h) provide such information as the Supplier may reasonably request and the Customer considers reasonably necessary, in order to carry out the Services in a timely manner;

5.2 If the Supplier's performance of its obligations under this Agreement is prevented or delayed by any act or omission of the Customer, its agents, subcontractors, consultants or employees then, without prejudice to any other right or remedy it may have, the Supplier shall be allowed an extension of time to perform its obligations equal to the delay caused by the Customer.

6. Charges and payment

6.1 In consideration for the provision of the Services by the Supplier, the Customer shall pay the Subscription Fees and the Charges in accordance with this clause 6 and the pricing table in the Service Contract. The Subscription Fees and the Charges shall be paid in £ pounds sterling, unless specified otherwise in the Service Contract.

6.2 The Supplier shall invoice the Subscription Fees and the Charges to the Customer at the intervals specified in the Service Contract. Each invoice shall include all reasonable supporting information required by the Customer to verify the accuracy of the invoice.

6.3 The Customer shall pay each invoice which is properly due and submitted to it by the Supplier, within 30 days of receipt, to a bank account nominated in writing by the Supplier unless otherwise stated in the Service Contract.

6.4 All amounts payable by the Customer are exclusive of amounts in respect of VAT or any other applicable equivalent tax chargeable for the time being. Where any taxable supply for VAT or similar tax purposes is made under the Service Contract by the Supplier to the Customer, the Customer shall, on receipt of a valid VAT invoice from the Supplier, pay to the Supplier such additional amounts in respect of VAT as are chargeable on the supply of the Services at the same time as payment is due for the supply of the Services.

6.5 The Supplier may increase the Subscription Fees and the Charges by up to 5% on an annual basis with effect from each anniversary of the date of the relevant Service Contract.

6.6 Without prejudice to any other right or remedy that it may have, if the Customer fails to pay the Supplier any sum due under this Agreement on the due date:

(a) the Customer shall pay interest on the overdue sum from the due date until payment of the overdue sum, whether before or after judgment. Interest under this clause will accrue each day at 4% a year above the Bank of England's base rate from time to time, but at 4% a year for any period when that base rate is below 0%; and

(b) the Supplier may suspend part or all of the Services until payment has been made in full.

6.7 All sums payable to the Supplier under this Agreement:

(a) are exclusive of VAT, and the Customer shall in addition pay an amount equal to any VAT chargeable on those sums on delivery of a VAT invoice; and

(b) shall be paid in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law).

7. Intellectual Property Rights

7.1 For the avoidance of doubt, all rights in and to the Compliance Assist Platform (whether such rights currently exist or as they may come into existence as a result of any further developments, modifications or reiterations of the same which take place during the Subscription Term) are owned by and retained by the Supplier and its licensors (where applicable).

7.2 The Supplier confirms that it has all the rights in relation the Compliance Assist Platform to enable it to provide the Services and grant all necessary rights to the Deliverables under, and in accordance with the terms of the Service Contract and this Agreement.

7.3 The Customer acknowledges and agrees that the Supplier and/or its licensors own all Intellectual Property Rights in the Compliance Assist Platform and the Services. Except as expressly stated herein, this Agreement does not grant the Customer any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trade marks (whether registered or unregistered), or any other rights in respect of the Compliance Assist Platform, the Services and the Deliverables.

7.4 The Supplier grants the Customer, or shall procure the direct grant to the Customer of, a fully paid-up, worldwide, non-exclusive, royalty-free licence during the term of the Service Contract for Authorised Users to access the Compliance Assist Platform for the purpose of receiving and using the Services and the Deliverables in its business.

7.5 The Customer shall not sub-license, assign or otherwise transfer the rights granted in clause 7.4:

(a) to other Customer Affiliates and customers;

(b) to third parties for the purpose of the Customer's receipt of services similar to the Services.

7.6 The Supplier warrants that the access and use of the Compliance Assist Platform and the supply of the Services by the Customer and the Authorised Users shall not infringe the rights, including any Intellectual Property Rights, of any third party.

7.7 The Supplier shall not be in breach of the warranty at clause 7.6 of this Agreement, and the Customer shall have no claim under the indemnity at clause 7.8 below, to the extent the infringement arises from:

(a) any modification of the Deliverables or Services, other than by or on behalf of the Supplier; or

(b) compliance with the Customer's specifications or instructions, where infringement could not have been avoided while complying with such specifications or instructions and provided that the Supplier shall notify the Customer if it knows or suspects that compliance with such specification or instruction may result in infringement.

7.8 Each party shall keep the other party indemnified in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, fines, legal and other professional fees and expenses awarded against or incurred or paid by the other party as a result of or in connection with any claim brought against that party for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt, use or supply of the Services and the Deliverables.

7.9 Each party shall:

(a) notify the other party in writing of any claim against it in respect of which it wishes to rely on the indemnity at clause 7.8 above (**IPRs Claim**);

(b) allow the other party, at its own cost, to conduct all negotiations and proceedings and to settle the IPRs Claim, always provided that that party shall obtain the other party's prior approval of any settlement terms, such approval not to be unreasonably withheld;

(c) provide the other party with such reasonable assistance regarding the IPRs Claim as is required by that party, subject to reimbursement by the other party of that party's costs so incurred;

(d) not, without prior consultation with the other party, make any admission relating to the IPRs Claim or attempt to settle it, provided that the Supplier considers and defends any IPRs Claim diligently, using competent counsel and in such a way as not to bring the reputation of the other party into disrepute.

7.10 In relation to the Customer Materials, the Customer:

(a) and its licensors shall retain ownership of all IPRs in the Customer Materials; and

(b) grants to the Supplier a fully paid-up, non-exclusive, royalty-free, non-transferable licence to copy and modify the Customer Materials for the term of this Agreement for the purpose of providing the Services to the Customer.

7.11 The Customer:

(a) warrants that the receipt and use in the performance of this Agreement by the Supplier, its agents, subcontractors or consultants of the Customer Materials shall not infringe the rights, including any Intellectual Property Rights, of any third party; and

(b) shall indemnify the Supplier against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred or paid by the Supplier arising out of or in connection with any claim brought against the Supplier, its agents, subcontractors or consultants for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt or use in the performance of this Agreement of the Customer Materials.

8. Data protection

8.1 For the purposes of this clause 8, the terms **controller**, **processor**, **data subject**, **personal data**, **personal data breach** and **processing** shall have the meaning given to them in the UK GDPR.

8.2 Both parties will comply with all applicable requirements of Applicable Data Protection Laws. This clause 8 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Applicable Data Protection Laws.

8.3 The parties have determined that, for the purposes of Applicable Data Protection Laws:

(a) the Supplier shall process the Customer Personal Data as processor on behalf of the Customer; and

(b) the Supplier shall act as controller of the Supplier Personal Data.

8.4 Should the determination in clause 8.3 change, the parties shall use all reasonable endeavours to make any changes that are necessary to this clause 8 and Schedule 3.

8.5 The Customer consents to, (and shall procure all required consents, from its personnel, representatives and agents, in respect of) all actions taken by the Supplier in connection with the processing of Supplier Personal Data, provided these are in compliance with the then-current version of the Supplier's privacy policy available at https://www.complianceassist.co.uk/privacy-policy/ (**Privacy Policy**). In the event of any inconsistency or conflict between the terms of the Privacy Policy and this agreement, the Privacy Policy will take precedence.

8.6 Without prejudice to the generality of clause 8.2, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Supplier Personal Data and Customer Personal Data to the Supplier or lawful collection of the same by the Supplier for the duration and purposes of this Agreement.

8.7 In relation to the Customer Personal Data, Schedule 1 sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of personal data and categories of data subject.

8.8 Without prejudice to the generality of clause 8.2, the Supplier shall, in relation to Customer Personal Data:

(a) process that Customer Personal Data only on the documented instructions of the Customer, which shall be to process the Customer Personal Data for the purposes set out in Schedule 1 (Processing, personal data and data subjects) unless the Supplier is required by Applicable Laws to otherwise process that Customer Personal Data (**Purpose**). Where the Supplier is relying on Applicable Laws as the basis for processing Customer Processor Data, the Supplier shall notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Provider from so notifying the Customer on important grounds of public interest. The Supplier shall inform the Customer if, in the opinion of the Supplier, the instructions of the Customer infringe Applicable Data Protection Laws;

(b) implement the technical and organisational measures set out in Schedule 1 to protect against unauthorised or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, which the Customer has reviewed and confirms are appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

(c) ensure that any personnel engaged and authorised by the Supplier to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

(d) assist the Customer insofar as this is possible (taking into account the nature of the processing and the information available to the Supplier), and at the Customer's cost and written request, in responding to any request from a data subject and in ensuring the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(e) notify the Customer without undue delay on becoming aware of a personal data breach involving the Customer Personal Data; and

(f) maintain records to demonstrate its compliance with this clause 8.

8.9 The Customer provides its prior, general authorisation for the Supplier to:

(a) appoint processors to process the Customer Personal Data, provided that the Supplier:

(i) shall ensure that the terms on which it appoints such processors comply with Applicable Data Protection Laws, and are consistent with the obligations imposed on the Supplier in this clause 8;

(ii) shall remain responsible for the acts and omission of any such processor as if they were the acts and omissions of the Supplier; and

(iii) shall inform the Customer of any intended changes concerning the addition or replacement of the processors, thereby giving the Customer the opportunity to object to such changes provided that if the Customer objects to the changes and cannot demonstrate, to the Supplier's reasonable satisfaction, that the objection is due to an actual or likely breach of Applicable Data Protection Law, the Customer shall indemnify the Supplier for any losses, damages, costs (including legal fees) and expenses suffered by the Supplier in accommodating the objection.

(b) transfer Customer Personal Data outside of the UK as required for the Purpose, provided that the Supplier shall ensure that all such transfers are effected in accordance with Applicable Data Protection Laws. For these purposes, the Customer shall promptly comply with any reasonable request of the Supplier, including any request to enter into standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the Commissioner from time to time (where the UK GDPR applies to the transfer).

8.10 Either party may, at any time on not less than 30 days' notice, revise this clause 8 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

8.11 The Supplier's liability for losses arising from breaches of this clause 8 is as set out in clause 10.2.

9. Confidentiality

9.1 Each party undertakes that it shall not at any time disclose to any person any confidential information concerning the business, affairs, customers, clients or suppliers of the other party or of any of that party's Affiliates, except as permitted by clause 9.3.

9.2 The Supplier may delete any confidential information in its custody in accordance with any Applicable Data Protection Law.

9.3 Each party may disclose the other party's confidential information:

(a) to its employees, officers, representatives, contractors, subcontractors or advisers who need to know such information for the purposes of exercising the party's rights or carrying out its obligations under or in connection with this Agreement. Each party shall ensure that its employees, officers, representatives, contractors, subcontractors or advisers to whom it discloses the other party's confidential information comply with this clause 9; and

(b) as may be required by law, a court of competent jurisdiction or any governmental or regulatory authority.

9.4 No party shall use the other party's confidential information for any purpose other than to exercise its rights and perform its obligations under or in connection with this Agreement.

10. Limitation of liability

10.1 Nothing in this agreement limits any liability which cannot legally be limited, including but not limited to liability for:

(a) death or personal injury caused by negligence; and

(b) fraud or fraudulent misrepresentation.

10.2 Subject to Clause 10.1 (liabilities which cannot legally be limited), and to the indemnity (for infringement of third party intellectual property rights) provided in clause 7.8 and for a failure to comply with its data processing obligations under clause 8 (which such liability shall be limited to the extent of the Supplier's relevant available insurance cover) the Supplier's total liability to the Customer whether in contract, tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with this Agreement shall be limited to the value of the total of the Subscription Fees and Charges paid and/or payable by the Customer over the 12 month period preceding the event that gave rise to the liability.

10.3 Subject to clauses 10.1 and 10.2 above, this clause 10.3 specifies the types of losses that are excluded:

(a) loss of profits;

(b) loss of sales or business;

(c) regulatory or other fines or penalties imposed or levied on the Customer by any competent authority in connection with the use of the Services;

(d) loss of agreements or contracts;

(e) loss of anticipated savings;

(f) loss of use or corruption of software, data or information;

(g) loss of or damage to goodwill; and

(h) indirect or consequential loss.

11. Termination

11.1 Without affecting any other right or remedy available to it, either party may terminate this Agreement with immediate effect by giving written notice to the other party if:

(a) the other party commits a material breach of any term of this Agreement and (if such breach is remediable) fails to remedy that breach within a period of 14 (fourteen) days after being notified in writing to do so;

(b) the other party repeatedly breaches any of the terms of this Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this Agreement;

(c) the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts;

(d) the other party commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with any of its creditors;

(e) the other party applies to court for, or obtains, a moratorium under Part A1 of the IA 1986;

(f) a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of the other party (being a company, limited liability partnership or partnership);

(g) an application is made to court, or an order is made, for the appointment of an administrator, or a notice of intention to appoint an administrator is given or an administrator is appointed, over the other party (being a company, partnership or limited liability partnership);

(h) the holder of a qualifying floating charge over the assets of that other party (being a company or limited liability partnership) has become entitled to appoint or has appointed an administrative receiver;

(i) a person becomes entitled to appoint a receiver over all or any of the assets of the other party or a receiver is appointed over all or any of the assets of the other party;

(j) a creditor or encumbrancer of the other party attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the other party's assets and such attachment or process is not discharged within 14 days;

(k) any event occurs, or proceeding is taken, with respect to the other party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clause 11.1(c) to clause 11.1(j) (inclusive);

(l) the other party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business; or

(m) the other party's financial position deteriorates so far as to reasonably justify the opinion that its ability to give effect to the terms of this agreement is in jeopardy.

11.2 For the purposes of clause 11.1(a), **material breach** means a breach (including an anticipatory breach) that is serious in the widest sense of having a serious effect on the benefit which the terminating party would otherwise derive from this Agreement or from a failure by the other party to meet any of its obligations. In deciding whether any

breach is material no regard shall be had to whether it occurs by some accident, mishap, mistake or misunderstanding.

11.3 Without affecting any other right or remedy available to it, the Supplier may terminate this agreement with immediate effect by giving written notice to the Customer if:

(a) the Customer fails to pay any amount due under this agreement on the due date for payment and remains in default not less than 14 days after being notified in writing to make such payment; or

(b) there is a change of Control of the Customer.

11.4 Without affecting any other right or remedy available to it, the Supplier may, at its sole discretion, suspend the provision of the Services if the Customer fails to pay any of its invoices in part or in full. Following such a suspension, the parties may agree to lift the suspension once the due payments have been made.

11.5 Without affecting any other right or remedy available to it, the Customer or the Supplier may terminate this Agreement on giving not less than 2 (two) months' written notice to the Supplier before the end of the applicable anniversary date of the relevant Service Contract.

12. Obligations on termination and survival

12.1 Obligations on termination or expiry

On termination or expiry of this Agreement:

(a) the Customer shall immediately pay to the Supplier all of the Supplier's outstanding unpaid invoices and interest and, in respect of the Services supplied but for which no invoice has been submitted, the Supplier may submit an invoice, which shall be payable immediately on receipt;

(b) the Supplier shall on request return any of the Customer Materials not used up in the provision of the Services.

12.2 Survival

(a) On termination or expiry of this Agreement, all existing Statements at Work shall terminate automatically.

(b) Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination or expiry of this Agreement shall remain in full force and effect.

(c) Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry.

13. Force majeure

13.1 **Force Majeure Event** means any circumstance not within a party's reasonable control including, without limitation:

(a) acts of God, flood, drought, earthquake or other natural disaster;

(b) epidemic or pandemic;

(c) terrorist attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict or any kind of special military operation, imposition of sanctions, embargo, or breaking off of diplomatic relations;

(d) nuclear, chemical or biological contamination or sonic boom;

(e) any law or any action taken by a government or public authority, including without limitation imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent;

(f) Extended interruption or failure of utility service.

13.2 Provided it has complied with clause 13.4, if a party is prevented, hindered or delayed in or from performing any of its obligations under this agreement by a Force Majeure Event (**Affected Party**), the Affected Party shall not be in breach of this agreement or otherwise liable for any such failure or delay in the performance of such obligations. The time for performance of such obligations shall be extended accordingly.

13.3 The corresponding obligations of the other party will be suspended, and its time for performance of such obligations extended, to the same extent as those of the Affected Party.

13.4 The Affected Party shall:

(a) as soon as reasonably practicable after the start of the Force Majeure Event but no later than 7 days from its start, notify the other party in writing of the Force Majeure Event, the date on which it started, its likely or potential duration, and the effect of the Force Majeure Event on its ability to perform any of its obligations under the Agreement; and

(b) use all reasonable endeavours to mitigate the effect of the Force Majeure Event on the performance of its obligations.

13.5 If the Force Majeure Event prevents, hinders or delays the Affected Party's performance of its obligations for a continuous period of more than 4 (four) weeks, the party not affected by the Force Majeure Event may terminate this Agreement by giving 4 (four) weeks' written notice to the Affected Party.

14. Assignment and other dealings

14.1 The Customer shall not assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under this Agreement.

14.2 The Supplier may at any time assign, mortgage, charge, delegate, declare a trust over or deal in any other manner with any or all of its rights under this Agreement.

15. Variation

No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

16. Waiver

16.1 A waiver of any right or remedy under this Agreement or by law is only effective if given in writing and shall not be deemed a waiver of any subsequent right or remedy.

16.2 A failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this agreement or by law shall prevent or restrict the further exercise of that or any other right or remedy.

17. Rights and remedies

The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

18. Severance

18.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

18.2 If any provision or part-provision of this agreement is deemed deleted under clause 18.1 the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

19. Entire agreement

19.1 This Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

19.2 Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this Agreement.

20. No partnership or agency

20.1 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

20.2 Each party confirms it is acting on its own behalf and not for the benefit of any other person.

21. Third party rights

21.1 This agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

21.2 The rights of the parties to rescind or vary this Agreement are not subject to the consent of any other person and for the avoidance of doubt the Customer and the Supplier may vary, terminate or rescind this Agreement without the consent of any Customer Affiliate.

22. Notices

22.1 Any notice or other communication given to a party under or in connection with this Agreement shall be in writing and shall be:

(a) delivered by hand or by pre-paid first-class post or other next Business Day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(b) sent by email to the address specified in the Service Contract.

22.2 Any notice or communication shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address;

(b) if sent by pre-paid first-class post or other next Business Day delivery services, at 9.00 am on the second Business Day after posting; or

(c) if sent by email, at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 22.2(c), business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

22.3 This clause does not apply to the service of any proceedings or any documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

22.4 A notice given under this Agreement is valid if sent by email.

23. Governing law

This 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 law of England and Wales.

24. Jurisdiction

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

This Agreement has been entered into on the date stated at the beginning of it.

Schedule 1

Data Processing Agreement

The terms used in this Data Processing Agreement shall have the meanings set forth in this Data Processing Agreement. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Appendices 1 and 2 form an integral part of this Data Processing Agreement.

Except where the context requires otherwise, references in this Data Processing Agreement to the Agreement are to the Agreement as amended by, and including, this Data Processing Agreement.

1. Definitions

In this Data Processing Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to EU Data Protection Laws; (b) laws of the United kingdom with respect to any Customer Personal Data in respect of any Customer Group Member is subject to UK Data Protection Laws and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to any other Data Protection Laws;

1.2 "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.3 "**Customer Group Member**" means Customer or any Customer Affiliate;

1.4 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Customer Group Member pursuant to or in connection with the Agreement;

1.5 "**Contracted Processor**" means Supplier or a Subprocessor;

1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.7 "**EEA**" means the European Economic Area;

1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.10 "**Restricted Transfer**" means:

1.10.1 a transfer of Customer Personal Data from any Customer Group Member to a Contracted Processor; or

1.10.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.3.3 or 12 below;

1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Supplier for Customer Group Members pursuant to the Agreement;

1.12 "**Standard Contractual Clauses**" means the standard contractual clauses set out in Appendix 3, amended by module, in that Appendix and under section 13.4;

1.13 "**Subprocessor**" means any person (including any third party and any Supplier Affiliate, but excluding an employee of Supplier or any of its sub-contractors) appointed by or on behalf of Supplier or any Supplier Affiliate to Process Personal Data on behalf of any Customer Group Member in connection with the Agreement; and

1.14 "**Supplier Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Supplier, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.15 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.16 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Roles of the Parties

2.1 Customer Group Member acts as the Controller.

2.2 Supplier and Supplier Affiliates act as the Processor.

3. Processing of Customer Personal Data

3.1 Supplier and each Supplier Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

3.1.2 not Process Customer Personal Data other than for the purpose of providing the Services specified in the Agreement unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Supplier or the relevant Supplier Affiliate shall to the extent permitted by Applicable Laws inform the relevant Customer Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Customer Group Member:

3.2.1 instructs Supplier and each Supplier Affiliate (and authorises Supplier and each Supplier Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Customer Personal Data; and

3.2.1.2 in particular, transfer Customer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Customer Affiliate.

3.2.3 has sole responsibility for the accuracy, quality and legality of the Customer Personal Data and the means by which the Customer Group Member acquired the Customer Personal Data.

3.3 Appendix 1 to this Data Processing Agreement sets out certain information regarding the Contracted Processors' Processing of the Customer Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Customer may make reasonable amendments to Appendix 1 by written notice to Supplier from time to time as Customer reasonably considers necessary to meet those requirements. Nothing in Appendix 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Data Processing Agreement.

4. Supplier and Supplier Affiliate Personnel

Supplier and each Supplier Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor, who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Supplier and each Supplier Affiliate has implemented and maintains a comprehensive written information security program that complies with Data Protection Laws and Appendix 2 of this Data Processing Agreement, including appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Appendix 2 and as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data.

5.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier and each Supplier Affiliate shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.3 In assessing the appropriate level of security, Supplier and each Supplier Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

6.1 Each Customer Group Member authorises Supplier and each Supplier Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

6.2 Supplier and each Supplier Affiliate may use the following Subprocessors, subject to Supplier and each Supplier Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4:

- Amazon Web Services (Data storage and infrastructure)
- Zoho (CRM and helpdesk)
- Experian (Verification service)
- Equifax (Verification service)
- Acuris (Adverse information screening)
- Au10tix (Physical ID Verification service)

Supplier shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor no later than 60 days prior to any such change. If, within 10 days of receipt of that notice, Customer notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, neither Supplier nor any Supplier Affiliate shall appoint (nor disclose any Customer Personal Data to) the proposed Subprocessor except with the prior written consent of Customer.

6.3 With respect to each Subprocessor, Supplier or the relevant Supplier Affiliate shall:

6.3.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Agreement;

6.3.2 ensure that the arrangement between on the one hand (a) Supplier, or (b) the relevant Supplier Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Data Processing Agreement and meet the requirements of article 28(3) of the GDPR;

6.3.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Supplier, or (b) the relevant Supplier Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Customer Group Member(s) (and Customer shall procure that each Customer Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.3.4 provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Data Processing Agreement) as Customer may request from time to time.

6.4 Supplier and each Supplier Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this Data Processing Agreement in place of Supplier.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Supplier and each Supplier Affiliate shall assist each Customer Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer Group Members' obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Supplier shall:

7.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Supplier shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Supplier shall notify Customer as soon as reasonably practicable upon Supplier or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow each Customer Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Supplier shall co-operate with Customer and each Customer Group Member and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Supplier and each Supplier Affiliate shall provide reasonable assistance to each Customer Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Customer Personal Data

Supplier and each Supplier Affiliate warrants that upon termination of the Agreement or upon request to securely delete or return Personal Data, comply with Customer Group Member's request, and securely delete existing copies unless applicable laws requires storage of the Customer Personal Data (in which case Supplier and each Supplier Affiliate will protect the confidentiality of the Customer Personal Data, will not actively Process the Customer Personal Data anymore, and will continue to comply with this Data Processing Agreement)

11. Audit rights

11.1 Subject to sections [11.2 to 11.4], Supplier and each Supplier Affiliate shall make available to each Customer Group Member on request all information necessary to demonstrate compliance with this Data Processing Agreement, and shall allow for and contribute to audits, including inspections, by any Customer Group Member or an auditor mandated by any Customer Group Member in relation to the Processing of the Customer Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Customer Group Members only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Customer or the relevant Customer Affiliate undertaking an audit shall give Supplier or the relevant Supplier Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer or the relevant Customer Affiliate undertaking an audit has given notice to Supplier or the relevant Supplier Affiliate that this is the case before attendance outside those hours begins; or

11.3.3 for the purposes of more than [one] audit or inspection, in respect of each Contracted Processor, in any [calendar year], except for any additional audits or inspections which:

11.3.3.1 Customer or the relevant Customer Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Supplier's or the relevant Supplier Affiliate's compliance with this Data Processing Agreement; or

11.3.3.2 A Customer Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Customer or the relevant Customer Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Supplier or the relevant Supplier Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Customer Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Customer Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 Supplier warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Supplier Affiliate, Supplier's or the relevant Supplier Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Data Processing Agreement hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Data Processing Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Data Processing Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

13.2 Nothing in this Data Processing Agreement reduces Supplier's or any Supplier Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Supplier or any Supplier Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Data Processing Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Data Processing Agreement, in the event of inconsistencies between the provisions of this Data Processing Agreement and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Data Processing Agreement, the provisions of this Data Processing Agreement shall prevail.

Changes in Data Protection Laws, etc.

13.4 Customer may:

13.4.1 by at least 30 (thirty) calendar days written notice to Supplier from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Data Processing Agreement which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Customer gives notice under section 13.4.1:

13.5.1 Supplier and each Supplier Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

13.5.2 Customer shall not unreasonably withhold or delay agreement to any consequential variations to this Data Processing Agreement proposed by Supplier to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Customer gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

13.7 Neither Customer nor Supplier shall require the consent or approval of any Customer Affiliate or Supplier Affiliate to amend this Data Processing Agreement pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Data Processing Agreement be invalid or unenforceable, then the remainder of this Data Processing Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement.

The nature and purpose of the Processing of Customer Personal Data

- Screening of parties to comply with applicable laws and regulations
- Any other Processing as stipulated as Services in the Agreement

The types of Customer Personal Data to be Processed

- Title
- First and last names
- Age
- Gender
- Date of birth
- Nationality
- Current address
- Previous address
- Telephone numbers
- Bank account details
- ID documentation
- Any other data required to comply with applicable laws and regulations.

The categories of Data Subject to whom the Customer Personal Data relates

Customers, business partners, vendors, employees, agents and advisors of Customer Group Member.

Owners, directors, shareholders, beneficial owners, controllers, employees and customers of customers, business partners or vendors of Customer Group Member.

The obligations and rights of Customer and Customer Affiliates

The obligations and rights of Customer and Customer Affiliates are set out in the Agreement and this Data Processing Agreement.

APPENDIX 2: List of Security Measures

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths
- Establishing access authorizations for employees and third parties
- Access control system (ID reader, magnetic card, chip card)
- Key management, card-keys procedures
- Door locking (electric door openers etc.)
- Security staff,
- Surveillance facilities, video/CCTV monitor, alarm system
- Securing decentralized data processing equipment and personal computers

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures
- ID/password security procedures
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Personal Data in accordance with their access rights, and that Customer Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures
- Control authorization schemes
- Differentiated access rights (profiles, roles, transactions and objects)
- Monitoring and logging of accesses
- Disciplinary action against employees who access Personal Data without authorization
- Reports of access
- Access procedure
- Change procedure
- Deletion procedure
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption
- Logging

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems
- Audit trails and documentation

6. Control of instructions

Technical and organizational measures to ensure that Customer Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Customer Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

APPENDIX 3: Contractual Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

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.

MODULE ONE: Transfer controller to controller

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 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 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 (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 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.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter 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.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter

under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

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

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(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. 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 (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.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[1] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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;

[1] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(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

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(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.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

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

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

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(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;

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until

required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that

prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: 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 _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 _____ (*specify Member State*).

(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.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

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: …

Signature and date: …

Role (controller/processor): …

2. …

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: …

Signature and date: …

Role (controller/processor): …

2. …

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

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.

.....

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

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

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

.....

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

.....

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

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

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

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

Address: …

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
…

2. …

International Data Transfer Addendum the the Standard Contractual Clauses

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		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

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

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						
2						
3						

4						

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:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

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

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

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

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

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

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the

inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

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

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

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

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

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

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