DATED 2026

(1) ETRADING SOFTWARE (UK BOND CTP) LTD

(2) [PARTNER]

ACCREDITED PARTNER AGREEMENT

CONTENTS

THIS AGREEMENT is made on [DATE]

BETWEEN:

(1) **ETRADING SOFTWARE (UK BOND CTP) LTD**, a company incorporated in England and Wales with registered number 16686242 and whose registered office is at Randall House, 6 Dowgate Hill, London, England, EC4R 2SU (the "**CTP**"); and

(2) **[●]**, a company incorporated in [●] with registered number [●] and whose registered office is at [●] (the "**Partner**"),

(each a "**Party**" and together the "**Parties**").

WHEREAS:

(A) The CTP has been appointed by the FCA as the provider of the Consolidated Tape.

(B) The CTP operates an Accredited Partner Programme under which qualifying organisations are granted accredited status to provide L1 Support to Licensees.

(C) The Partner has applied for and been granted accredited status under the Accredited Partner Programme, subject to the terms and conditions of this Agreement.

(D) This Agreement sets out the terms on which the Partner is authorised to hold itself out as a member of the Accredited Partner Programme and provide L1 Support to Licensees (and to access the CTP's tooling and data for that purpose).

IT IS AGREED as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless the context otherwise requires, the following terms shall have the following meanings:

Accredited Partner Data	data made available by the CTP to the Partner via the Diagnostics API, including API technical logs, FIX 5.0 session logs, user login success/failure events and session status information, in each case strictly relating to the Partner's contracted Licensees and/or internal users (as applicable);
Accredited Partner Programme	the CTP's accredited partner programme pursuant to which organisations are authorised to provide L1 Support;
Administrative Functions	the defined set of operational actions available to the Partner via the AP Portal, as published by the CTP from time to time. The scope of Administrative Functions is set by the CTP;

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 (with "Control" having the meaning given in section 1124 of the UK's Corporation Tax Act 2010);
AP Portal	the integrated web-based interface provided by the CTP to members of the Accredited Partner Programme;
Business Day	A day other than a Saturday, Sunday or public holiday in England when banks in London are open for business;
Confidential Information	the contents of this Agreement and all information in whatever form received or obtained by a Party (the "**Receiving Party**") from, or on behalf of, the other Party (the "**Disclosing Party**") as a result of, or in connection with, this Agreement other than: (a) any information which was rightfully in the possession of the Receiving Party prior to the disclosure by the Disclosing Party and acquired on a non-confidential basis from sources other than the Disclosing Party; and (b) any information which is in the public domain otherwise than as a result of a breach of this Agreement by the Receiving Party, and, for the avoidance of doubt, the Accredited Partner Data is Confidential Information of the CTP;
Consolidated Tape	the UK Bond Consolidated Tape developed and made available by the CTP;
CTP Board	the board of the CTP, responsible for governance and oversight of the Consolidated Tape operation, including final determination within the CTP governance framework in respect of accreditation decisions in respect of the Accredited Partner Programme;
CTP GUI	the display-only graphical user interface provided by the CTP, accessible via the AP Portal, enabling members of the Accredited Partner Programme to view bond trade data for the purpose of handling data-related client queries;
CTP Status Dashboard	the operational status view available via the AP Portal, providing all members of the Accredited Partner Programme with real-time visibility of planned Downtime, change notifications and systemic incidents affecting the Consolidated Tape service;
Data Protection Legislation	any law applicable from time to time relating to the processing of personal data and/or privacy, as in force at the date of this Agreement or as reenacted, applied, amended, superseded, repealed or consolidated, including without limitation, the UK GDPR, the UK Data Protection Act 2018, the EU GDPR (as the case may be) and the Privacy and Electronic Communications (EC

	Directive) Regulations 2003, in each case including any legally binding regulations, directions and orders issued from time to time under or in connection with any such law;
Diagnostics API	the purpose-built REST API provided by the CTP via AWS API Gateway, giving members of the Accredited Partner Programme controlled access to Accredited Partner Data;
Downtime	the CTP tooling being generally unavailable to members of the Accredited Partner Programme (excluding, for the avoidance of doubt, any inability of the Partner to access tooling on account of Partner-side connectivity issues);
FCA	the UK's Financial Conduct Authority;
Good Industry Practice	in relation to any activity and under any circumstances, the exercise of a high degree of skill, diligence, prudence, risk management, quality management and foresight as can be expected from the top-tier providers of the same or similar services;
Incident	means a failure of an aspect of the Consolidated Tape service to function as expected or required in accordance with the CTP's arrangements with the FCA;
Initial Term	has the meaning given in Clause 21.1;
Intellectual Property Rights	all trade marks, service marks, trade and business names, domain names, design rights, copyright, moral rights, rights in databases, rights in inventions, patents, logos, rights to sue for passing off, trade secrets, rights in know-how, rights in Confidential Information and other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted (and rights to claim priority from) such rights (including renewals or extensions) and all rights or forms of protection having equivalent or similar effect to any of the foregoing which subsist or will subsist now or in the future in any part of the world;
L1 Support	first-line Licensee-facing assistance provided by the Partner in respect of a Licensee's use of, and connectivity to, the Consolidated Tape service, as more particularly described in Clause 5;
Licensees	persons to whom the CTP (or any authorised redistributor) provides the Consolidated Tape;

Market Hours	the hours during which the UK bond market is open for trading, being 08:00 to 18:00 London time on Business Days;
Renewal Term	has the meaning given in Clause 21.2;
Security Incident	any actual or suspected: (i) breach of Accredited Partner Data; (ii) unauthorised access to CTP systems or infrastructure; (iii) compromise of the Partner's systems used to access the Diagnostics API or store Accredited Partner Data; or (iv) incident that in the CTP's reasonable opinion poses an immediate risk to the integrity, availability or confidentiality of the Consolidated Tape or its users' data;
Technical Specifications	the Accredited Partner Programme Technical Specifications as published by the CTP on its website at www.ets-connect.co.uk and via the AP Portal, as amended from time to time in accordance with Clause 10; and
Term	the Initial Term together with any Renewal Term(s).

1.2 Unless the context otherwise requires, references in this Agreement to:

1.2.1 any of the masculine, feminine and neuter genders shall include other genders;

1.2.2 the singular shall include the plural and vice versa;

1.2.3 a "**clause**", "**Schedule**" or "**paragraph**" shall (unless otherwise stated) be construed as a reference to a clause of or Schedule to this Agreement or to a paragraph of the relevant Schedule;

1.2.4 a "**person**" shall be construed as a reference to any individual, firm, company (including, without limitation, a limited liability company), corporation, government, state or agency of a state or any association or partnership (whether or not having separate legal personality) of two or more of the foregoing;

1.2.5 a "**company**" shall include a reference to any body corporate;

1.2.6 the term "**including**" shall be construed as meaning "**including without limitation**";

1.2.7 any statute or statutory provision shall be construed as a reference to such statute or statutory provision (including all instruments, orders or regulations made thereunder or deriving validity therefrom) as in force at the date of this Agreement and as subsequently amended, substituted, re-enacted or consolidated; and

1.2.8 any time or date shall be construed as a reference to the time or date prevailing in England.

1.3 The headings in this Agreement are for convenience only and shall not affect its meaning.

1.4 The Schedules to this Agreement form part of this Agreement and shall have the same force and effect as if expressly set out in the body of this Agreement.

2. PURPOSE AND RELATIONSHIP

2.1 This Agreement governs the relationship between the CTP and the Partner in connection with the Partner's provision of L1 Support to Licensees.

2.2 The Partner acts independently and is not an agent of the CTP. Nothing in this Agreement shall create or be deemed to create a partnership, joint venture, agency or employment relationship between the Parties.

2.3 The CTP retains full accountability for the operation, integrity and resilience of the Consolidated Tape at all times.

2.4 The Partner shall not hold itself out as having any authority to bind the CTP or to make any representation or commitment on the CTP's behalf.

3. ACCREDITATION GRANT

3.1 Subject to the terms of this Agreement, the CTP grants the Partner non-exclusive accredited status under the Accredited Partner Programme and permits the Partner to provide L1 Support to Licensees.

3.2 No fees are payable by either Party to the other Party under this Agreement.

3.3 The Partner shall be free to determine its own fee arrangements with its Licensee clients for the provision of L1 Support.

3.4 The Partner shall provide L1 Support to Licensees:

3.4.1 in compliance with applicable laws and regulations;

3.4.2 in compliance with the relevant policies of the CTP and the FCA (as provided to the Partner by the CTP from time to time);

3.4.3 in compliance with Good Industry Practice;

3.4.4 in compliance with all instructions issued by the CTP from time to time, provided that all such instructions are reasonable and compliance will not cause the Partner to be in breach of this Agreement;

3.4.5 in compliance with the terms of the arrangements entered into between the Partner and the relevant Licensees; and

3.4.6 using appropriately qualified, supervised and trained personnel.

3.5 The Partner acknowledges that membership of the Accredited Partner Programme is non-exclusive and open to any person that meets the objective, proportionate and transparent criteria published by the CTP from time to time. It does not confer any preferential rights over the Consolidated Tape.

3.6 The Partner shall assist the CTP with responding to (and complying with) any relevant FCA investigation or enquiry.

4. CERTIFICATION REQUIREMENTS

4.1 The Partner acknowledges that it has been admitted to the Accredited Partner Programme on the basis that it has demonstrated (and on the condition that it will continue to demonstrate) capability across three pillars (as further described in the remainder of this Clause 4):

4.1.1 controls and security;

4.1.2 operational capability; and

4.1.3 governance and oversight.

4.2 The Partner must hold and maintain at least one certification from each of the following categories as a condition of accreditation:

4.2.1 controls and security: ISO 27001 or SOC 2 Type II; and

4.2.2 operational capability: ISO/IEC 20000-1:2018 or CMMI for Services (CMMI-SVC) Level 3.

4.3 The Partner shall ensure that each certification it obtains and maintains pursuant to Clause 4.2 directly covers its provision of L1 Support and, at a minimum:

4.3.1 in respect of ISO 27001 or SOC 2 Type II, covers:

a) the Partner's systems and infrastructure used to access the Diagnostics API;

b) the Partner's storage and processing of Accredited Partner Data;

c) the Partner's helpdesk and support tooling used to deliver L1 Support; and

d) all of the Partner's personnel involved in delivering L1 Support to Licensees;

4.3.2 in respect of ISO/IEC 20000-1:2018, covers:

a) the Partner's service management processes used to deliver L1 Support;

b) the Partner's incident management, escalation and problem management processes; and

c) the Partner's service desk function itself;

4.3.3 in respect of CMMI-SVC Level 3, covers:

a. the Partner's service management processes used to deliver L1 Support;

b. the Partner's incident management, escalation and problem management processes; and

c. the Partner's service desk function itself.

4.4 Where the Partner obtains CMMI-SVC Level 3 pursuant to Clause 4.2.2, the appraisal must have been conducted within the preceding 36 months by a Certified CMMI Lead Appraiser through a registered CMMI Institute Partner.

4.5 At least once each calendar year, the Partner shall provide the CTP with a written report setting out the precise scope of the relevant certification(s) held by the Partner pursuant to Clause 4.2, in each case demonstrating that such certification(s) meet the requirements set out in Clause 4.3 (and, if applicable, Clause 4.4). If the CTP (acting reasonably and in good faith) considers any such document insufficient to demonstrate compliance with the relevant requirements of this Agreement, the CTP may notify the Partner, and the Partner shall submit a revised report without undue delay.

4.6 If, at any time during the Term: (i) the Partner ceases to hold at least one certification from each category listed in Clause 4.2 which meets the requirements set out in Clause 4.3 (and, if applicable, Clause 4.4); (ii) the Partner fails to provide any report required by Clause 4.5; or (iii) the Partner fails to provide a revised report required by Clause 4.5 to the CTP's reasonable satisfaction, then the CTP may provide the Partner with written notice of such occurrence requiring remediation within 30 days. If the Partner fails to remedy the issue within 30 days of receiving such written notice, such failure shall be considered an irremediable material breach of this Agreement.

5. SCOPE OF L1 SUPPORT

5.1 The CTP hereby authorises the Partner to provide L1 Support to Licensees in respect of connectivity and usage issues.

5.2 L1 Support includes responding to Licensee queries, diagnosing Licensee-side connectivity and configuration issues, assisting with API session management and onboarding, performing predefined Licensee-scoped remediation actions (such as session re-initialisation) where permitted by the CTP, and escalating matters outside the scope of L1 Support (such as those listed in Clause 5.3) to the CTP in accordance with Clause 7.

5.3 L1 Support does not include any intervention in, or diagnosis of, platform-level systems, data integrity, or issues affecting more than one Licensee's environment (other than where the Partner is a redistributor of the Consolidated Tape and all affected Licensees are contracted by the Partner in its capacity as redistributor).

5.4 The Partner shall comply with the Technical Specifications when delivering L1 Support and when accessing or using any CTP systems, tools or data.

6. SERVICE LEVELS

6.1 All L1 Support provided by the Partner must, where relevant, meet the minimum service levels set out in the column "*Partner time to resolution or escalation*" in Schedule 1. The Parties acknowledge that the column "*CTP time to resolution*" is included for reference only.

6.2 The Partner acknowledges that the service levels set out in Schedule 1 are structured as a percentage of the CTP's own incident resolution obligations, in accordance with the operational level agreement framework set out in ISO/IEC 20000-1:2018.

6.3 The Partner must use its best endeavours to resolve all L1 Support tickets within its competence within the timeframes set out in Schedule 1. Without prejudice to the foregoing, if the Partner cannot resolve an L1 Support ticket within the relevant timeframe, it must escalate the ticket to the CTP immediately via the escalation path set out in Clause 7, with full ticket details in accordance with the Technical Specifications.

6.4 The Partner's performance will be measured against the service levels by the CTP and reported as part of the performance reporting obligations set out in Clause 18.

7. ESCALATION TO THE CTP

7.1 The Partner must maintain a clear and documented escalation process to the CTP's back-end support function, in accordance with the Technical Specifications.

7.2 The Partner must escalate to the CTP, without undue delay and in any event within 24 hours (or such shorter period as provided for in Schedule 1), any issue that falls outside its L1 Support scope, including any suspected data quality issue, platform outage, or incident that may affect more than one Licensee. The CTP will publish and maintain escalation procedures and contact details for this purpose, which shall be accessible via the AP Portal.

7.3 All escalations made by the Partner must comply with the escalation template and process set out in the Technical Specifications.

8. ACCESS TO ACCREDITED PARTNER DATA AND TOOLING

8.1 To enable the Partner to provide L1 Support, the CTP will provide the Partner with access to Accredited Partner Data via the Diagnostics API. The Partner will have no access to platform-wide logs, non-relevant Licensee data, or any data beyond what is necessary for its support role.

8.2 The CTP will provide the Partner with access to the AP Portal, which shall deliver the following capability areas:

8.2.1 access to the licence details and all user accounts (both human and programmatic) of the Licensees to whom the Partner has contracted to provide L1 Support;

8.2.2 the CTP Status Dashboard;

8.2.3 Administrative Functions; and

8.2.4 CTP GUI access.

8.3 The CTP reserves the right to deliver the capabilities listed in Clause 8.2 via separate interfaces if required by its technical architecture, provided that the functional scope is not reduced.

8.4 All access to the AP Portal, Diagnostics API and Accredited Partner Data by the Partner must be in accordance with the Technical Specifications.

8.5 The CTP shall ensure that the CTP-provided tooling (including the AP Portal and Diagnostics API) is available (i.e., not subject to Downtime) for at least 99.99% of the time during Business Days in each calendar month, calculated on a monthly basis and excluding any periods of planned Downtime for maintenance notified via the CTP Status Dashboard. The Partner shall have no liability to the CTP (including in relation to service levels) for any losses directly caused by Downtime provided: (i) no workaround to the relevant Downtime is reasonably available to the Partner; and (ii) the Partner notifies the CTP within [30] minutes of becoming aware of tooling unavailability which may result from Downtime.

8.6 The CTP shall defend the Partner against any claim that the Partner's use of CTP-provided tooling in accordance with this Agreement infringes any third party's Intellectual Property Rights and shall indemnify the Partner for any amounts awarded against the Partner in judgment or settlement of such claims, provided that: (i) the CTP is given prompt notice of any such claim; (ii) the Partner does not make any admission, or otherwise attempt to compromise or settle the claim and provides reasonable co-operation to the CTP in the defence and settlement of such claim, at the CTP's expense; and (iii) the CTP is given sole authority to defend or settle the claim.

8.7 In the defence or settlement of any claim subject to the indemnity in Clause 8.6, the CTP may procure the right for the Partner to continue using the affected tooling, replace or modify the affected tooling so that it becomes non-infringing or, if such remedies are not reasonably available, terminate this Agreement on 2 Business Days' notice to the Partner without any additional liability or obligation to pay liquidated damages or other additional costs to the Partner.

8.8 In no event shall the CTP be liable to the Partner under Clause 8.6 to the extent that the alleged infringement is based on: (i) a modification of the tooling by anyone other than the CTP; (ii) the Partner's use of the tooling in a manner contrary to the instructions given to the Partner by the CTP; (iii) the Partner's use of the tooling after becoming aware of the alleged or actual infringement; or (iv) the Partner's breach of this Agreement.

8.9 Clauses 8.6 - 8.8 and Clause 20.2 state the Partner's sole and exclusive rights and remedies, and the CTP's entire obligations and liability, for any claim subject to the indemnity in Clause 8.6.

9. ONBOARDING

9.1 Prior to going live:

9.1.1 the CTP will provision the Partner with access to a test environment replicating the production AP Portal and Diagnostics API; and

9.1.2 the Partner shall complete a formal technical onboarding process including credential provisioning, test environment integration, and a go-live readiness sign-off conducted by the CTP, in accordance with the Technical Specifications.

9.2 The Partner may not access the production environment until go-live sign-off has been granted by the CTP. The CTP shall not unreasonably withhold or delay go-live sign-off. If the CTP declines to grant go-live sign-off, it shall provide the Partner with written reasons for its decision.

10. CHANGE MANAGEMENT

10.1 The CTP may make changes to the AP Portal (including the CTP Status Dashboard and the CTP GUI), Diagnostics API, Administrative Functions, authentication infrastructure or Technical Specifications from time to time. The CTP shall notify the Partner at least 90 days in advance of implementation of material changes, except where the CTP reasonably considers a shorter notice period to be necessary for security, regulatory or operational reasons (in which case the CTP shall provide such shorter period of notice).

10.2 Where reasonably practicable, the CTP will consult with members of the Accredited Partner Programme (which may include the Partner) via the CTP Board before implementing material changes to the AP Portal, Diagnostics API, Administrative Functions, authentication infrastructure or Technical Specifications.

10.3 If any change to the Technical Specifications materially increases (or would materially increase) the Partner's cost of complying with the Technical Specifications, the Partner may terminate this Agreement on written notice to the CTP.

10.4 The CTP will maintain a published change log accessible via the AP Portal recording all changes to the tooling suite and the effective date of each change.

11. INCIDENT NOTIFICATION

11.1 In addition to the status information available via the CTP Status Dashboard, the CTP will provide direct proactive notification to the Partner if it becomes aware of any Priority 1 Incident or Priority 2 Incident (each as defined in Schedule 1) affecting the Consolidated Tape service, in accordance with the Technical Specifications.

11.2 Notifications made by the CTP pursuant to Clause 11.1 shall:

11.2.1 be made without undue delay following incident classification by the CTP;

11.2.2 include, where known by the CTP, details of: (i) the nature and scope of the incident; (ii) the affected services; (iii) the estimated time to resolution; and (iv) any recommended actions for the Partner to communicate to its contracted Licensees; and

11.2.3 be delivered via email to the designated contact address registered by the Partner at onboarding. The Partner is responsible for maintaining an accurate designated contact address and for ensuring appropriate internal distribution of CTP incident notifications.

11.3 Following issuance of notifications pursuant to Clause 11.1, the CTP shall provide the Partner with updates at regular intervals until the incident is resolved.

11.4 The CTP will publish a post-incident summary on the AP Portal following resolution of any Priority 1 Incident (as defined in Schedule 1).

12. TRAINING AND DOCUMENTATION

12.1 The CTP will make the following documentation accessible via the AP Portal:

12.1.1 Diagnostics API technical specification including endpoint definitions, authentication guide, data schemas, rate limits and error codes;

12.1.2 AP Portal user guide covering all available functions;

12.1.3 Administrative Functions specification describing each permitted action, its scope, conditions of use and any client impact considerations;

12.1.4 escalation procedures and contact details for the CTP back-end support function;

12.1.5 onboarding and offboarding checklists; and

12.1.6 a change log of all material updates to the tooling suite.

12.2 The CTP will notify the Partner of material updates to any documentation listed in Clause 12.1 via the AP Portal and by email to the Partner's designated contact address.

12.3 The CTP will make available a structured onboarding training programme for new members of the Accredited Partner Programme.

12.4 The Partner is responsible for ensuring all personnel delivering L1 Support on behalf of the Partner are appropriately trained and familiar with current CTP documentation and the Technical Specifications.

13. USE OF ACCREDITED PARTNER DATA

13.1 The Partner may use Accredited Partner Data solely for the purpose of providing L1 Support to its contracted Licensees.

13.2 Without prejudice to Clause 13.1, the Partner may not use Accredited Partner Data for any commercial purpose, internal analytics, product development or any purpose beyond its role as a member of the Accredited Partner Programme. For the avoidance of doubt, this Clause 13.2 shall not: (i) prevent the Partner from analysing data about its own performance (or its own clients) to improve its provision of L1 Support; or (ii) affect any rights granted to the Partner under any other arrangement (including any arrangement under which the Partner redistributes the Consolidated Tape).

13.3 Both Parties will comply with applicable Data Protection Legislation. To the extent that Accredited Partner Data contains personal data (as defined in applicable Data Protection Legislation), (i) the Partner acts as an independent controller in respect of its own processing; and (ii) if the Partner is located outside the UK or the European Economic Area, Schedule 2 shall apply between the Parties.

13.4 The Partner must not retain Accredited Partner Data beyond what is necessary for the delivery of L1 Support.

14. CONFIDENTIALITY

14.1 Subject to Clause 14.2, each Receiving Party shall treat in confidence all Confidential Information and shall not use Confidential Information for a purpose other than for the exercise of its rights, or the performance of its obligations, under this Agreement.

14.2 Notwithstanding the provisions of Clause 14.1, a Receiving Party may disclose Confidential Information:

14.2.1 to its own personnel, solely to the extent required for the proper performance of this Agreement or to enable it to receive professional advice in respect of its rights and obligations under this Agreement (conditional upon any such personnel being informed of the confidential nature of the Confidential Information and the Receiving Party procuring that such personnel comply with equivalent obligations of confidentiality as those set out in this clause 14); and

14.2.2 to the extent that such Confidential Information is required to be disclosed by applicable laws or is to be disclosed to the FCA or any other regulator, in each case provided that the other party (if it is lawful to do so) is notified in advance that such disclosure is to be made (such advance notice to be given as soon as reasonably practicable).

14.3 Following termination of this Agreement, the Receiving Party shall, without undue delay, procure that all Confidential Information in its possession or under its control is deleted or

destroyed (save to the extent and for so long as any applicable laws or terms of the Agreement require such Confidential Information to be retained) and shall confirm in writing to the Disclosing Party that it has done so.

14.4 Each Receiving Party undertakes to apply to the Confidential Information at least the same security measures and degree of care as it applies to its own confidential information.

14.5 The CTP will not use (or permit any person to use) data collected from the Partner under this Agreement other than: (i) for the purposes of operating the Accredited Partner Programme; (ii) for the purposes of creating, developing, maintaining and distributing the Consolidated Tape; and/or (iii) as required in order to comply with applicable laws.

14.6 The obligations in this Clause 14 shall survive termination of this Agreement.

15. SECURITY INCIDENTS

15.1 The Partner shall notify the CTP without undue delay (and in any event within 24 hours) upon becoming aware of any actual or suspected Security Incident.

15.2 All notifications made pursuant to Clause 15.1 must include all relevant information reasonably available to the Partner at the time, including details of:

15.2.1 the nature of the incident;

15.2.2 affected systems;

15.2.3 potential impact on Accredited Partner Data; and

15.2.4 any steps already taken to contain the incident.

15.3 The Partner must cooperate fully with the CTP in investigating and remedying any Security Incident.

15.4 The Partner may make public factual statements regarding Security Incidents (e.g., regarding unavailability of the Consolidated Tape and/or L1 Support) but may not make any public statement regarding the cause of any Security Incident (including any attribution of fault) without the prior written consent of the CTP, except where disclosure is required by applicable laws or to the FCA, the Information Commissioner's Office or any other competent regulator or authority, in which case the Partner shall notify the CTP in advance of such disclosure where it is lawful and reasonably practicable to do so.

16. AUDIT

16.1 During the Term and for a period of two years thereafter, the Partner shall maintain complete and accurate records of its provision of L1 Support.

16.2 On request, the Partner shall provide the CTP and any auditors of or other advisers to the CTP with access to and copies of any of the Partner's operational controls, systems, records

and other documents relating to provision of L1 Support as may be reasonably required in order for the CTP to:

16.2.1 comply with any audit undertaken or commissioned by the FCA;

16.2.2 satisfy any obligation (or exercise any right) under applicable laws;

16.2.3 verify the Partner's compliance with the terms of this Agreement; and

16.2.4 verify the accuracy of information provided by the Partner to the CTP in relation to this Agreement.

16.3 The Partner shall:

16.3.1 on request (but no more frequently than once in any 12-month period), promptly (and in any event within 14 calendar days) complete any audit questionnaire provided to it by the CTP; and

16.3.2 provide all reasonable co-operation, access and assistance in relation to any audit undertaken pursuant to this Clause 16.

16.4 In relation to audits undertaken pursuant to Clause 16.2, the CTP shall:

16.4.1 not undertake more than one audit in any 12-month period and shall provide the Partner with at least 14 days' advance notice of any audit to be undertaken, in each case unless: (i) the CTP reasonably suspects a Security Incident, regulatory breach or breach of this Agreement has occurred; and/or (ii) required by the FCA;

16.4.2 use reasonable endeavours to minimise disruption to the Partner; and

16.4.3 ensure that any auditors or other advisers to the CTP engaged in relation to any audit are: (i) bound by obligations of confidentiality; and (ii) not competitors of the Partner.

16.5 Each Party shall bear its own costs and expenses incurred in respect of compliance with its obligations under this Clause 16, unless the audit identifies any material non-compliance by the Partner with the terms of the Agreement, in which case the Partner shall reimburse the CTP for its reasonable costs and expenses.

16.6 Any material failure by the Partner to cooperate with any audit undertaken pursuant to this Clause 16 shall be a material breach of this Agreement.

17. NO MISREPRESENTATION

17.1 The Partner must not represent itself as acting on behalf of the CTP or create any impression that it is the CTP or an authorised representative of the CTP. All Licensee-facing communications made by the Partner must make clear that support is provided by the Partner in its own capacity as a member of the Accredited Partner Programme.

17.2 The CTP hereby grants the Partner a non-exclusive, non-transferable, revocable right during the Term to use the CTP's name, trade marks and logos solely to identify itself as a member of the Accredited Partner Programme in connection with the delivery and promotion of its L1 Support services, subject to any brand guidelines issued by the CTP from time to time.

17.3 The Partner must not modify the CTP's trade marks, use them in conjunction with any other mark or logo, or use them in any way that could damage the goodwill or reputation of the CTP.

17.4 The Partner acknowledges that all goodwill arising from the Partner's use of the CTP's name, trade marks and logos pursuant to Clause 17.2 shall vest in and belong exclusively to the CTP.

18. PERFORMANCE REPORTING

18.1 The CTP will generate monthly performance metrics for the Partner from its own Diagnostics API logs and audit data. These CTP-generated metrics will cover areas including ticket escalation rates, AP Portal access patterns, incident response timeliness and service availability.

18.2 The Partner will provide a monthly self-reported performance return to the CTP within 10 Business Days of the end of each calendar month, covering its helpdesk volumes, resolution times, adherence to service levels and any material issues or contextual factors affecting its performance during the period.

18.3 Both the CTP-generated and Partner self-reported metrics will be included as part of the CTP's regulatory reporting framework on a monthly basis.

18.4 A consolidated summary of the performance metrics of members of the Accredited Partner Programme will be published publicly on an aggregated and anonymised basis on a quarterly basis, such that no individual member is identified or identifiable.

18.5 The CTP's records will be treated as authoritative (with regards to performance of a Party's obligations under this Agreement) in the event of any discrepancy between the CTP-generated and Partner self-reported data sets. If the Partner reasonably considers any of the CTP's records to be incorrect, it may notify the CTP in writing. The CTP shall consider any such notification in good faith and, if appropriate, shall rectify its records.

19. INTELLECTUAL PROPERTY RIGHTS

19.1 All Intellectual Property Rights in and to the AP Portal, Diagnostics API, CTP GUI, CTP Status Dashboard, Accredited Partner Data, Technical Specifications and all related documentation remain vested in the CTP and its licensors.

19.2 The Partner is granted no Intellectual Property Rights under this Agreement other than a non-exclusive, non-transferable, revocable licence during the Term to: (i) access and use

the AP Portal, Diagnostics API, CTP GUI, CTP Status Dashboard, Accredited Partner Data, Technical Specifications and related documentation for the sole purpose of delivering L1 Support to its contracted Licensees; and (ii) use the CTP's name, trade marks and logos in accordance with Clause 17.2.

19.3 Nothing in this Agreement shall transfer or assign any Intellectual Property Rights from one Party to the other Party.

20. LIABILITY

20.1 The Partner shall indemnify and keep indemnified the CTP against any losses, costs, claims, damages or expenses (including reasonable legal costs) arising out of or in connection with:

20.1.1 any action taken by the Partner using the Administrative Functions, whether taken incorrectly, negligently, outside permitted scope or without appropriate authorisation from the affected Licensee;

20.1.2 any breach by the Partner of its obligations under this Agreement (including the Technical Specifications), including failure to escalate any Incident within the applicable timeframe set out in Schedule 1;

20.1.3 any misuse of Accredited Partner Data by the Partner or any unauthorised disclosure of Confidential Information by the Partner;

20.1.4 any act or omission of the Partner's personnel, subcontractors or agents in connection with this Agreement;

20.1.5 any claim brought against the CTP or its licensors or redistributors by a Licensee or third party arising from the Partner's delivery of, or failure to deliver, L1 Support; and/or

20.1.6 any regulatory fines issued to the CTP as a direct result of the Partner's non-compliance with this Agreement.

20.2 Subject to Clause 20.4, each Party's total aggregate liability to the other under or in connection with this Agreement, whether in contract, tort (including negligence) or otherwise, shall be limited to £5 million.

20.3 Subject to Clause 20.4, neither Party shall have any liability to the other for any:

20.3.1 indirect, consequential, special or economic loss;

20.3.2 loss of revenue;

20.3.3 loss of profit; or

20.3.4 loss of anticipated savings,

in each case howsoever arising.

20.4 Nothing in this Agreement shall limit or exclude:

20.4.1 either Party's liability for death or personal injury caused by negligence;

20.4.2 either Party's liability for fraud or fraudulent misrepresentation;

20.4.3 either Party's liability for gross negligence or wilful misconduct; or

20.4.4 any liability that cannot be excluded or limited by applicable law.

20.5 The Partner acknowledges that the Administrative Functions available via the AP Portal are provided as a controlled operational tool and that, except to the extent provided in Clause 8.5, the CTP shall have no liability for any loss arising from any action taken by the Partner using the Administrative Functions.

21. TERM AND TERMINATION

21.1 This Agreement shall commence on the date of this Agreement and shall continue for an initial period of 12 months (the "**Initial Term**").

21.2 Following the Initial Term, this Agreement shall automatically renew for successive periods of 12 months (each a "**Renewal Term**"), subject to ongoing compliance with this Agreement (including the certification requirements in Clause 4), unless terminated in accordance with this Clause 21.

21.3 Either Party may terminate this Agreement at any time by giving not less than 90 days' written notice to the other Party.

21.4 The CTP may serve the Partner with written notice to terminate this Agreement (and thereby the Partner's membership of the Accredited Partner Programme) if:

21.4.1 any Security Incident occurs;

21.4.2 any regulatory breach occurs in connection with this Agreement or its subject matter;

21.4.3 directed or required to do so by the FCA;

21.4.4 the Partner persistently breaches the service levels set out in Schedule 1;

21.4.5 the Partner: (i) becomes unable to pay its debts; (ii) enters into liquidation (except for the purposes of a solvent amalgamation or reconstruction); (iii) applies for or obtains a moratorium; (iv) makes an arrangement with its creditors; (v) has a receiver, administrator or administrative receiver appointed over all or any of its assets; (vi) ceases or threatens to cease trading or is dissolved; (vii) takes or suffers to be taken any similar action in

consequence of a debt; or (viii) is subject to any procedure equivalent to any of the preceding matters in any other jurisdiction; or

21.4.6 the Partner commits a material breach of its obligations under this Agreement and (where the breach is capable of being remedied) that breach has not been remedied within 30 days after receipt of notice giving reasonable particulars of the breach and requiring the Partner to remedy it.

21.5 Any termination notice served by the CTP pursuant to Clause 21.4 shall:

21.5.1 if not challenged by the Partner pursuant to Clause 22.1, terminate this Agreement with effect from the date 20 Business Days after service of the termination notice; or

21.5.2 if challenged by the Partner pursuant to Clause 22.1, have such effect as determined by the CTP Board pursuant to Clause 22.3.

21.6 The CTP may suspend this Agreement (and thereby the Partner's membership of the Accredited Partner Programme) on immediate written notice to the Partner if: (i) any Security Incident occurs; (ii) any regulatory breach occurs in connection with this Agreement or its subject matter; (iii) directed or required to do so by the FCA; or (iv) the Partner persistently breaches the service levels set out in Schedule 1. Any suspension of this Agreement may last as long as the CTP reasonably deems appropriate and shall be without prejudice to the CTP's right to terminate this Agreement pursuant to Clause 21.4 in relation to the same trigger event.

21.7 The Partner may terminate this Agreement immediately by written notice to the CTP if the CTP: (i) becomes unable to pay its debts; (ii) enters into liquidation (except for the purposes of a solvent amalgamation or reconstruction); (iii) applies for or obtains a moratorium; (iv) makes an arrangement with its creditors; (v) has a receiver, administrator or administrative receiver appointed over all or any of its assets; (vi) ceases or threatens to cease trading or is dissolved; (vii) takes or suffers to be taken any similar action in consequence of a debt; or (viii) is subject to any procedure equivalent to any of the preceding matters in any other jurisdiction.

21.8 The Partner may terminate this Agreement immediately by written notice to the CTP if the CTP commits a material breach of its obligations under this Agreement and (where the breach is capable of being remedied) that breach has not been remedied within 30 days after receipt of notice giving reasonable particulars of the breach and requiring the CTP to remedy it.

21.9 On termination or revocation of the Partner's accreditation (including termination or suspension of this Agreement) for any reason:

21.9.1 the Partner shall immediately cease providing L1 Support;

21.9.2 the Partner's access to the AP Portal, Diagnostics API and all Accredited Partner Data will cease immediately; and

21.9.3 the CTP will immediately revoke the Partner's credentials, removing access to the AP Portal, Diagnostics API and all associated interfaces,

for the avoidance of doubt, in the case of suspension of this Agreement, these matters will be restored promptly following suspension.

21.10 The Partner shall, within 30 days of termination or revocation of its accreditation:

21.10.1 delete or destroy all Accredited Partner Data in its possession and confirm the same in writing to the CTP;

21.10.2 cease all use of any CTP branding, trade marks or references to its status as a member of the Accredited Partner Programme; and

21.10.3 notify its contracted Licensees that it is no longer a member of the Accredited Partner Programme and direct them to the CTP for alternative support arrangements,

for the avoidance of doubt, this Clause 21.10 shall not: (i) be triggered by suspension of the Agreement pursuant to Clause 21.6; or (ii) affect any rights granted to the Partner under any other arrangement (including any arrangement under which the Partner redistributes the Consolidated Tape).

21.11 The CTP may maintain records of all access made by the Partner to the AP Portal, the Diagnostics API and all associated interfaces (both during the term of this Agreement and following its termination).

21.12 Clauses 13, 14, 15, 16, 20, 21.10 and 33 shall survive termination of this Agreement.

22. CHALLENGE PROCESS

22.1 Subject to Clause 22.2, the Partner (acting reasonably and in good faith) may challenge any of the following actions if made by the CTP in connection with this Agreement:

22.1.1 the CTP notifies the Partner pursuant to Clause 4.5 that it considers a document to be insufficient to demonstrate compliance with the certification requirements of this Agreement;

22.1.2 the CTP declines to grant go-live sign-off pursuant to Clause 9.2;

22.1.3 the CTP serves a notice of termination of this Agreement pursuant to Clause 21.3 or 21.4; or

22.1.4 the CTP notifies the Partner of changes to the AP Portal, Diagnostics API, Administrative Functions, authentication infrastructure or Technical Specifications pursuant to Clause 10.1.

22.2 Any challenge made by the Partner must be made by submitting written grounds of challenge to the CTP Board within 20 Business Days of the action in question.

22.3 Following submission of any challenge in accordance with Clause 22.1.3:

22.3.1 the CTP Board will review the matter in its sole discretion and issue a final determination in accordance with the CTP governance framework within 20 Business Days;

22.3.2 the CTP's proposed action will be stayed pending determination, unless the CTP reasonably considers that it would pose a risk to the integrity of the service or its users' data; and

22.3.3 following a final determination being made by the CTP Board, both Parties will comply with the determination (without prejudice to their rights at law and under applicable regulations, including the right to bring legal claims).

23. ASSIGNMENT / SUBCONTRACTING

23.1 Subject to the further provisions of this Clause 23, neither Party shall, without the prior consent of the other Party, assign, mortgage, charge or declare a trust over any of its rights, or sub-contract, delegate or otherwise seek to transfer any of its obligations, under this Agreement.

23.2 The CTP may assign or transfer its rights and obligations under this Agreement to any successor operator of the Consolidated Tape without the Partner's consent, provided that the CTP gives the Partner written notice of such assignment or transfer.

23.3 The Partner may provide L1 Support using personnel of its Affiliates, provided: (i) the Partner provides the CTP with prior written notice (including the identity of each relevant Affiliate); (ii) the CTP has not objected to the Partner's use of such personnel; and (iii) the relevant Affiliates and personnel (as applicable) are covered by the certifications held by the Partner in accordance with Clauses 4.2 and 4.3. For the avoidance of doubt, the Partner shall be liable for all acts and omissions of its Affiliates and their personnel.

24. NOTICES

24.1 Any notice to be given by a Party under or in connection with this Agreement must be in English, in writing and delivered or sent to the following address in accordance with this Clause 24 (or such other address for service as the recipient Party may notify to the other Party from time to time giving not less than 30 days' prior notice in accordance with this Clause 24):

24.1.1 Notices for the CTP:

Attention: [*insert name of individual/position*]

Address: [*insert address*]

Email: [*insert email address*]

[Copy of notice to be sent to: [*name*] at [*address, email*]]

24.1.2 Notices for the Partner:

Attention: [*insert name of individual/position*]

Address: [*insert address*]

Email: [*insert email address*]

[Copy of notice to be sent to: [*name*] at [*address, email*]]

24.2 Notices must be served by one of the following methods:

24.2.1 by hand, which shall be deemed served upon delivery if delivered during Market Hours or at the start of Market Hours on the next Business Day if delivered at any other time;

24.2.2 by prepaid first class post or airmail post (if the recipient is not in the same country as the sender), which shall be deemed served at the start of Market Hours on the second Business Day following the day on which it was posted; or

24.2.3 by email, which shall be deemed served at the start of Market Hours on the next Business Day after transmission, provided that: (i) by close of Market Hours on the next Business Day after transmission, the Party serving the notice has not received a notification indicating that the email has failed to reach the recipient; and (ii) a copy of the notice is also despatched to the recipient using a method described in clause 24.2.1 or 24.2.2 no later than close of Market Hours on the next Business Day after transmission.

25. VARIATIONS AND WAIVERS

25.1 Subject to Clause 10, no variation of this Agreement shall be effective unless made in writing, signed by or on behalf of each of the Parties and expressed to be such a variation.

25.2 No failure or delay by any Party or time or indulgence given in exercising any remedy or right under or in relation to this Agreement shall operate as a waiver of the same, nor shall any single or partial exercise of any remedy or right preclude any further exercise of the same or the exercise of any other remedy or right.

25.3 No waiver by any Party of any requirement of this Agreement, or of any remedy or right under this Agreement, shall have effect unless given in writing and signed by such Party. No waiver of any particular breach of the provisions of this Agreement shall operate as a waiver of any repetition of such breach.

26. FURTHER ASSURANCE

At its own expense, each Party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, execute and deliver such documents and perform such acts as may be reasonably required for the purpose of giving full effect to this Agreement.

27. SEVERANCE

If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, the remaining provisions of this Agreement shall continue in full force and effect and 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.

28. RIGHTS OF THIRD PARTIES

Save as otherwise expressly provided in this Agreement, no provisions of this Agreement which confer rights upon any third party shall be enforceable pursuant to the Contracts (Rights of Third Parties) Act 1999 by any such third party.

29. NO PARTNERSHIP

This Agreement shall not create, nor shall it be construed as creating, any partnership or joint venture between the Parties.

30. ENTIRE AGREEMENT

30.1 This Agreement contains the entire agreement and understanding of the Parties and supersedes all prior agreements, promises, assurances, understandings or arrangements (both oral and written) relating to the subject matter of this Agreement (and any such document).

30.2 Each Party acknowledges that it is entering into this Agreement without reliance on any undertaking, warranty or representation given by or on behalf of the other Party (whether made innocently or negligently) other than as expressly contained in this Agreement, provided that nothing in this clause shall limit or exclude the liability of either Party for fraud or fraudulent misrepresentation.

31. COSTS

Save as otherwise expressly provided in this Agreement or any agreement to be entered into in connection herewith, each Party shall pay its own costs and expenses incurred in connection with the preparation, negotiation, execution and implementation of this Agreement.

32. COUNTERPARTS

This Agreement may be executed as two counterparts (which may be by electronic execution, including in PDF, JPEG or other similar format or using a recognised electronic document signing platform) and execution by each Party of any one such counterpart shall constitute due execution of this Agreement.

33. GOVERNING LAW AND JURISDICTION

33.1 This Agreement and any non-contractual obligations arising out of or in connection with this Agreement shall be governed by, and construed in accordance with, the laws of England and Wales.

33.2 Each Party irrevocably agrees to submit to the exclusive jurisdiction of the courts of England and Wales in respect of any claim or matter (including any non-contractual claim or matter) arising out of or in connection with this Agreement or the legal relationships established by this Agreement.

THIS AGREEMENT has been duly executed on the date first stated above.

SIGNED by _____)
for and on behalf of)
ETRADING SOFTWARE (UK BOND CTP) LTD) _____
Director

SIGNED by _____)
for and on behalf of)
[PARTNER]) _____
Director

SCHEDULE 1

SERVICE LEVELS

Incident level	Description	Partner time to resolution or escalation	CTP time to resolution
"**Priority 1 Incident**"	means an Incident which, in the reasonable opinion of the CTP, has caused, or may cause: • a complete loss or severe disruption to the Consolidated Tape service; • a complete loss or severe disruption of business-critical functionality in any part of the Consolidated Tape service; • a high level of reputational damage impacting public confidence in the FCA; • the publication (by suppliers or the media) of security vulnerabilities that could severely impact the Consolidated Tape service; • the FCA otherwise determines the Incident has an 'Impact' of 1 (or the Incident would otherwise be considered a Priority 1 Incident under the agreement between the CTP and the FCA); or • no workaround is available.	Thirty (30) minutes	Two (2) hours
"**Priority 2 Incident**"	means an Incident which, in the reasonable opinion of the CTP, has caused or has the potential to cause: • a complete loss of, or severe disruption to, the Consolidated Tape service; • a high level of reputational damage impacting public confidence in the FCA; • alerts from security systems (including but not limited to firewalls, intrusion detection systems and Internet gateways) that, in the opinion of the CTP, require further investigation; • the FCA otherwise determines the Incident has an 'Impact' of 2 (or the Incident would otherwise be considered a Priority 2 Incident under the agreement between the CTP and the FCA); or • a workaround is not available or is difficult to implement.	One (1) hour	Four (4) hours
"**Priority 3 Incident**"	means an Incident which, in the reasonable opinion of the CTP, has caused or has the potential to cause: • reputational damage to the FCA (but not a high level of reputational damage); • several (between 2 and 35) Licensee reports of viruses, phishing emails or other security concerns reported as individual Incidents of as a collective group; • the FCA otherwise determines the Incident has an 'Impact' of 3 (or the Incident would otherwise be considered a Priority 3 Incident under the agreement between the CTP and the FCA); or • a workaround is available.	Three (3) hours	Ten (10) hours
"**Priority 4 Incident**"	means an Incident which, in the reasonable opinion of the CTP has the potential to have a minor adverse impact on the provision of the Consolidated Tape service to Licensees, including: • a minor issue which, whilst inconvenient, has an agreed workaround to alleviate the impact to the Licensees; • where a single Licensee reports viruses, phishing emails or other security concerns; • which in each case will not cause any reputational damage to the FCA;	Ten (10) hours	Twenty (20) hours

	• the FCA otherwise determines the Incident has an 'Impact' of 4 (or the Incident would otherwise be considered a Priority 4 Incident under the agreement between the CTP and the FCA); or • all users have workarounds.		

Notes

1. The Partner shall take a cautious approach to assigning urgency, impact and Priority to an Incident and apply the most serious category that is appropriate for that Incident.
2. For the purposes of the table above, "resolution" means either: (i) the root cause of the Incident has been remedied and the Consolidated Tape service has been fully restored; (ii) the Consolidated Tape service has been restored and a workaround has been provided in relation to the Incident deemed acceptable by the CTP (and the FCA); (iii) the relevant solution to the Incident is to be provided in a scheduled release, and the solution is provided in that release.
3. The "*Partner time to resolution or escalation*" begins when the Licensee raises the ticket with the Partner.

SCHEDULE 2

CONTROLLER-TO-CONTROLLER UK INTERNATIONAL DATA TRANSFER AGREEMENT

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA 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 and signatures

Start date	[•]	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: eTrading Software (UK Bond CTP) Ltd Trading name (if different): N/A Main address (if a company registered address): Randall House, 6 Dowgate Hill, London, England, EC4R 2SU Official registration number (if any) (company number or similar identifier): 16686242	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): [•]	Full Name (optional): [•]

	Job Title: [●] Contact details including email: [●]	Job Title: [●] Contact details including email: [●]
Importer Data Subject Contact		Job Title: [●] Contact details including email: [●]
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: [●] Date of signature: [●] Full name: [●] Job title: [●]	Signed for and on behalf of the **Importer** set out above Signed: [●] Date of signature: [●] Full name: [●] Job title: [●]

Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☒ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☒ Importer is a Controller ☐ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)

Whether UK GDPR applies to the Importer	☐ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: Accredited Partner Agreement Date of agreement: [•] Parties to the agreement: [•] Reference (if any): [•] **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: [•] Date of agreement: [•] Parties to the agreement: [•] Reference (if any): [•] **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: [•] Date of agreement: [•] Parties to the agreement: [•] Reference (if any): [•]
Term	The Importer may Process the Transferred Data for the following time period: ☐ the period for which the Linked Agreement is in force ☐ time period:

	☒ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	☐ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. ☒ the Parties can end the IDTA before the end of the Term by serving: 3 months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☐ Importer ☐ Exporter ☒ neither Party
Can the Importer make further transfers of the Transferred Data?	☐ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☒ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☐ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: [•]

	The Parties must review the Security Requirements at least once: ☐ each _____ month(s) ☐ each quarter ☐ each 6 months ☒ each year ☐ each _____ year(s) ☐ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☐ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☒ none of the above ☐ set out in:

	And: ☐ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☐ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Purpose	☐ The Importer may Process the Transferred Data for the following purposes: ☐ The Importer may Process the Transferred Data for the purposes set out in: In both cases, any other purposes which are compatible with the purposes set out above. ☐ The purposes will update automatically if the information is updated in the Linked Agreement referred to. ☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

Security of Transmission	[●]
Security of Storage	[●]

Security of Processing	
Organisational security measures	[•]
Technical security minimum requirements	[•]
Updates to the Security Requirements	☐ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☒ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	[•]
(i) Extra technical security protections	[•]
(ii) Extra organisational protections	[•]
(iii) Extra contractual protections	[•]

Part 3: Commercial Clauses

Commercial Clauses	No commercial clauses apply. This IDTA is entered into in connection with the Accredited Partner Agreement dated [●].

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

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

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA 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.

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

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

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 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 IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is

appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

(a) a description of the nature of the Importer Personal Data Breach;

(b) (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

(c) likely consequences of the Importer Personal Data Breach;

(d) steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

(e) contact point for more information; and

(f) any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

(a) notify the third party receiver of the breach and suspend sending it Transferred Data; and

(b) if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA 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 IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

(a) the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

(b) the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);

- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	**Legal definition (this is how this word or phrase must be interpreted in the IDTA)**
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: • a territory; • one or more sectors or organisations within a third country; • an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 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 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
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.
Without Undue Delay	Without undue delay, as that phase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.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 5.4 of those Mandatory Clauses.