BCS GROUP MASTER SERVICE AGREEMENT - DATA SHARING SCHEDULE

This Data Sharing Schedule ("**Schedule**") forms part of the BCS Group Master Service Agreement. Words and definitions used in this Data Sharing Schedule will unless defined separately below or the context otherwise requires, bear the meanings given to them in the Agreement.

AGREED TERMS

1 DEFINITIONS

"Agreed Purpose" has the meaning given to it in clause 2 of this Schedule.

"Commissioner" means the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

"Criminal Offence Data" means Personal Data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the DPA 2018 (or other applicable Data Protection Legislation).

"Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in the UK including the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) ("**UK GDPR**"); the Data Protection Act 2018 (and regulations made thereunder) ("**DPA 2018**") and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

Controller, **Processor**, **Information Commissioner**, **Data Subject** and **Personal Data**, **Processing** and **appropriate technical and organisational** measures will have the meanings given to them in the Data Protection Legislation.

"Data Sharing Code" means the Information Commissioner's statutory data sharing code of practice which came into force on 5 October 2021, as updated or amended from time to time.

"**IDTA"** means the Information Commissioner's international data transfer agreement for the transfer of personal data from the UK, appended as Annex 1 to this Schedule.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

"Shared Personal Data" means the Personal Data to be shared between the parties under clause 3 of this Schedule.

"Special Categories of Personal Data" means the categories of Personal Data set out in the Data Protection Legislation.

"Subject Rights Request" means the exercise by a data subject of their rights under the Data Protection Legislation.

"Supervisory Authority" means the relevant supervisory authority in the territories where the parties to this Schedule are established (other than the Information Commissioner).

2 Purpose

2.1 This Schedule sets out the framework for the sharing of **Personal Data** when one **Controller** (the Data Discloser) discloses Personal Data to an independent **Controller** (the Data Receiver/s) in relation to each Service provided under an Order

Form. It defines the principles and procedures that the parties will adhere to and the responsibilities the parties owe to each other.

2.2 The parties agree to only Process Shared Personal Data, as described in Clause 3 of this Schedule for the following purposes:

Service	**Agreed Purpose**
ORGANISATIONAL MEMBERSHIP SCHEME	setting up membership and granting the Client's staff access to MyBCS (being the online portal for BCS members on www.bcs.org); **Additional Purposes** to enable BCS to use the Shared Data in an anonymised form for the following purposes: carrying out research including the preparation of white papers and market trends; identifying capability or market gaps with a view to informing decision to develop new products to address such gaps; promoting the importance of professionalism in the IT industry and the need to improve capability; and preparing event programmes in relation to professionalism in the IT industry.
ROLEMODEL*PLUS* AND CONSULTANCY SERVICES	granting the Client's employees access to RoleModel*plus* and provision of the Consultancy Services.
CPD MODULES	If applicable to the CPD Module, to contact learners via email to: a) provide them with access to the BCS Group platform so that they can take their examination; and b) confirm the results of such examination to the Client.
APPRENTICESHIPS	(a) assessing the work produced by the apprentice; (b) contact the apprentice or their employer (c) appraise the employer and apprentice of readiness of apprentice to undergo End-Point Assessment; (d) share data with the training provider; (e) share data with an Authorised Body for audit and validation purposes; (f) share data with the specified apprenticeship management platform as set out in the Operations Manual; (g) share the results with the apprentices; and (h) provide apprentices with BCS membership.
PROFESSIONAL CERTIFICATIONS	(a) assessing the work produced by the apprentice; (b) contact the apprentice or their employer (c) appraise the employer and apprentice of readiness of apprentice to undergo End-Point Assessment; (d) share data with the training provider; (e) share data with an Authorised Body for audit and validation purposes; (f) share data with the specified apprenticeship management platform as set out in the Operations Manual; and (g) share the results with the apprentices.
EDUCATION QUALIFICATIONS	(a) registering learners onto the relevant ICDL, Skills Builder, Compass or BCS Qualification programmes; (b) providing learners with access to online learning materials, diagnostic tools, assessments and related systems; (c) administering and invigilating assessments, including scheduling, identity checks, and recording assessment outcomes; (d) issuing results, certificates and digital badges to learners and, where appropriate, sharing outcomes with the Client; (e) supporting delivery and learner progress, including service updates, technical support and responding to learner or centre enquiries; (f) monitoring course engagement, assessment performance and

	progression for quality assurance and regulatory compliance purposes; (g) sharing required learner data with BCS, regulatory bodies, technology partners, and approved service providers as necessary for delivery, validation, audit or certification.

The parties will not Process Shared Personal Data in a way that is incompatible with the purposes described in this Clause (**Agreed Purpose**).

2.3 Each party will appoint a single point of contact who will have the appropriate skill level/role to be responsible for complying with the Data Protection Legislation and this Schedule ("**SPoC"**) who will work together to reach an agreement with regards to any issues arising from the data sharing. The point of contact for the BCS Group is Owen Field, Data Protection Officer, dataprivacy@bcs.uk.

3 Shared Personal Data

The following types of Personal Data will be shared between the parties during the Term of this Agreement:

Service	**Types of Data**
ORGANISATIONAL MEMBERSHIP SCHEME	a) Identification data (name, surname, date of birth); and b) Contact data (email address, postal address, telephone number).
ROLEMODEL*PLUS* AND CONSULTANCY SERVICES	a) Identification data (name, surname, date of birth) b) Contact data (email address, postal address, telephone number) c) Role profiles; and d) Team name.
CPD MODULES	If, applicable: a) Identification data (name); b) Contact data (email address); c) Online course progress tracking; and d) Examination result.
APPRENTICESHIPS	a) Apprentice title, first name and surname; b) Apprentice date of birth; c) Apprentice gender; d) Any reasonable adjustments required for the Apprentice; e) Unique Learner number; f) Apprenticeship Learning Aim Reference Service (LARS); g) BCS Membership information; h) Apprentice email address i) Apprentice Home address; j) Apprentice phone number; k) Statements from apprenticeship assessor or moderators; and l) Candidate portfolio including projects, evidence of work, exam results.
PROFESSIONAL CERTIFICATIONS	a) Candidate title, first name and surname; b) Any reasonable adjustments required for the Candidate; c) Candidate Home address; d) Qualification registered for; e) Trainer name; f) Outcome (pass/fail, Percentage or grade); g) Invigilator name(s); h) Proof of identification; and i) Candidate email address.
EDUCATION QUALIFICATIONS	The following data is required or generated in respect of each BCS Qualification undertaken by a Learner: a) Learner Name; b) Learner Date of Birth; c) Learner Gender;

	d) Learner House Number;
	e) Learner Postcode;
	f) Assessment Units(s) taken;
	g) Assessment Unit(s) Outcome;
	h) Date(s) Assessment(s) taken;
	i) Name of Authorised Tester(s);
	j) Date Certificate issued (if relevant);
	k) Syllabus Version;
	l) Method of Testing used;
	m) Number of Guided Learning Hours completed; and
	n) Method of Guided Learning Hours completed
	
	Special Category Data: Learner Ethnicity
	
	The following data is required or generated in respect of each DMP undertaken by a Learner:
	a) Learner Name;
	b) Syllabus Version/Name of Exam;
	c) Method of Testing used;
	d) Date of Birth;
	e) Learner House Number;
	f) Learner Postcode;
	g) Assessment Units(s) taken;
	h) Assessment Unit(s) Outcome;
	i) Date(s) Assessment(s) taken;
	j) Name of Authorised Tester(s); and
	k) Date Certificate issued (if relevant) – following the Learner passing the exam or achieving all prerequisites.

4 Lawful, fair and transparent processing

4.1 Each party will ensure that it Processes the Shared Personal Data fairly and lawfully in accordance with Clause 4.2 of this Schedule during the Term of this Agreement.

4.2 Each party will ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Data.

4.3 The Data Discloser will, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Data, the legal basis for such purposes and such other information as is required by the Data Protection Legislation including:

(a) if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer.

4.4 The Data Receiver undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Data, the legal basis for such purposes and such other information as is required by the Data Protection Legislation. including:

(a) if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer.

5 Data quality

5.1 The Data Discloser will ensure that before the Effective Date, Shared Personal Data is accurate and that it has appropriate internal procedures in place for the Data Receiver to sample Shared Personal Data prior to the Effective Date and it will update the same if required prior to transferring the Shared Personal Data.

5.2 Shared Personal Data must be limited to the Personal Data described in Clause 3 of this Schedule.

6 Data subjects' rights

6.1 In the event that a party received a Subject Rights Request relating to Personal Data held by the other party, the receiving party will instruct the Data Subject to contact the other party directly to fulfil their Subject Rights Request. There will be no obligation on either party to notify or assist the other party in relation to such Subject Rights Request.

7 Data retention and deletion

7.1 The Data Receiver will not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purpose.

7.2 Notwithstanding Clause 7.1 of this Schedule, the parties will continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective industry.

8 Security and training

8.1 The parties undertake to have in place throughout the Term of the Agreement appropriate technical and organisational security measures to:

(a) prevent:

(i) unauthorised or unlawful processing of the Shared Personal Data; and

(ii) the accidental loss or destruction of, or damage to, the Shared Personal Data

(b) ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

(ii) the nature of the Shared Personal Data to be protected.

8.2 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures together with any other applicable Data Protection Legislation and guidance and have entered into confidentiality agreements relating to the Processing of Personal Data.

8.3 The level, content and regularity of training referred to in Clause 8.2 of this Schedule will be proportionate to the staff members' role, responsibility and frequency with respect to their handling and Processing of the Shared Personal Data.

9 Personal data breaches and reporting procedures

9.1 The parties will each comply with its obligation to report a Personal Data Breach to the Information Commissioner or appropriate Supervisory Authority and (where applicable) Data Subjects under the Data Protection Legislation and will

each inform the other party of any Personal Data Breach irrespective of whether there is a requirement to notify the Information Commissioner or any Supervisory Authority or Data Subject(s).

9.2 The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

10 Resolution of disputes with data subjects or the Supervisory Authority

10.1 In the event of a dispute, complaint or claim brought by a Data Subject or the Information Commissioner concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes, complaints or claims, and will cooperate with a view to settling them amicably in a timely fashion.

10.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

10.3 Each party will abide by a decision of a competent court of the Data Discloser's country of establishment or of the Information Commissioner.

11 Warranties

11.1 Each party warrants and undertakes that it will:

(a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Personal Data processing operations.

(b) Respond within a reasonable time and as far as reasonably possible to enquiries from the Information Commissioner or relevant Supervisory Authority in relation to the Shared Personal Data.

(c) Respond to Subject Rights Requests in accordance with the Data Protection Legislation, including where necessary (i) advising the other party of any step(s) it should reasonably take in this regard; and (ii) where the legitimate ground relied upon is a Data Subject's consent, the timely operation of an effective procedure if such consent is withdrawn.

(d) Where applicable, maintain registration with the Information Commissioner and all relevant Supervisory Authorities to process all Shared Personal Data for the Agreed Purpose.

(e) Take all appropriate steps to ensure compliance with the security measures set out in clause 8 above.

11.2 The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Data to the Data Receiver and it will ensure that the Shared Personal Data is accurate.

12 Indemnity

The Client will indemnify the BCS Group (as applicable to the Service) and hold the BCS Group (as applicable to the Service) harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Schedule.

13 Additional Purposes

The Client agrees that the BCS Group is authorised to anonymise any Shared Data used for Additional Purposes Shared Data and to use it, in such anonymised form, for the Additional Purposes only.

14 International Data Transfers

14.1 The Client must not transfer or otherwise process the Personal Data outside the UK or EEA without obtaining the BCS Group's prior written consent.

14.2 Where such consent is granted, the Client may only process, or permit the processing, of the Personal Data outside the UK or EEA under the following conditions:

(a) the Client is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals;

(b) the Client participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Client (and, where appropriate, the BCS Group) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR; or

(c) the parties comply with the IDTA in Annex 1 to this Schedule.

ANNEX 1 – IDTA

ico.
Information Commissioner's Office

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	(As per Order Form)	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	(As per Order Form)	(As per Order Form)
Key Contact	dataprivacy@bcs.uk	(As per Order Form)
Importer Data Subject Contact	(As per Order Form)	(As per Order Form)

Signatures confirming each Party agrees to be bound by this IDTA	(As per Order Form)	(As per Order Form)

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	(As per Order Form)
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: ____ 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 **ONLY IF UNDER AN ORDER FOR EDUCATION QUALIFICTIONS**

	☐ 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 **ALL OTHER SERVICES** ☐ 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 the attached agreement referenced in Table 2 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	

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:

(a) Part one: Tables;

(b) Part two: Extra Protection Clauses;

(c) Part three: Commercial Clauses; and

(d) 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:

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

(b) 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):

(a) the same copy of this IDTA;

(b) 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;

(c) 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:

(a) 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;

(b) 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;

(c) 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

(d) 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:

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

(b) 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):

(a) 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

(b) 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:

(a) singular or plural words or people, also includes the plural or singular of those words or people;

(b) 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

(c) 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:

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

(b) 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:

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

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

8.3 The Importer must:

(a) 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");

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

(c) 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

(d) 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:

(a) the Importer Information is accurate;

(b) 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:

(a) 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

(b) 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:

(a) 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;

(b) 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

(c) 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:

(a) comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

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

(c) 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:

(a) only Process the Transferred Data for the Purpose;

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

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

(d) 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;

(e) 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

(f) 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:

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

(b) 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:

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

(b) 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

(c) 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:

(a) 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

(b) 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:

(a) 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,

(b) 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

(c) 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:

(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.

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:

(a) 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

(b) the third party has been added to this IDTA as a Party; or

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

(d) 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

(e) 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:

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

(b) 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;

(c) 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:

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

(b) 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;

(c) in clear and plain English that is easy to understand; and

(d) in an easily accessible form

together with

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

(f) 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:

(a) rectify inaccurate or incomplete Transferred Data;

(b) erase Transferred Data if it is being Processed in breach of this IDTA;

(c) cease using it for direct marketing purposes; and

(d) 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:

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

(b) 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

(c) 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:

(a) it is unable to reasonably verify the identity of an individual making the request; or

(b) 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

(c) 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 (b) 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:

(a) 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

(b) 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:

(a) contain all the terms and conditions agreed by the Parties; and

(b) 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:

(a) it only applies in so far as it explicitly waives specific rights or remedies;

(b) 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

(c) 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:

(a) has breached this IDTA; or

(b) 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:

(a) the Exporter must suspend sending Transferred Data to the Importer;

(b) 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

(c) 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:

(a) at the end of the Term stated in Table 2: Transfer Details; or

(b) 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;

(c) at any time that the Parties agree in writing that it will end; or

(d) 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:

(a) its direct costs of performing its obligations under the IDTA; and/or

(b) 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:

(a) 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;

(b) 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:

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

(b) 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

(c) 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):

(a) the Exporter must stop sending Transferred Data to the Importer; and

(b) 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;

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

(d) 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(b), 12.1(c), 12.1(d), 12.1(e) and 12.1(f) (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:

(a) Party One's breach of this IDTA; and/or

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

(c) 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(f) (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 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.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.
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(a), 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.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. 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.
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

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.