**Schedule 5c**

1. schedule 5C - DATA PROTECTION

 University (as controller) to Controller (with international Transfers to a restricted country)

1. DATA PROTECTION
2. DEFINITIONS

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| "**Applicable Law**" | means all applicable laws, statutes, enactments, regulations, declarations decrees, directives, legislative enactments, orders, binding decisions of a competent Court or Tribunal, regulations, rules, regulatory policies, guidelines, codes, other binding restrictions, regulatory permits and licences applicable under law which are in force from time to time during the term of the Agreement, including the rules, codes of conduct, codes of practice, practice requirements and accreditation terms stipulated by any regulatory authority or body to which a Party is subject from time to time as the same are amended, consolidated, modified, re-enacted or replaced; |
| **"Controller"** |  means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; |
| "**Data Exporter**" | means a Party making or proposing to make a transfer of Personal Data which is a Restricted Transfer;  |
| "**Data Importer**" | means a Party in receipt of Personal Data as a result of a Restricted Transfer; |
| "**Data Originator**" | means the Party from whom the Shared Data originates; |
| "**Data Processing Particulars**" | means, in relation to any Processing under this Agreement:the subject matter and duration of the Processing;the nature and purpose of the Processing;the type of Personal Data being Processed; andthe categories of Data Subjects;as set out in Appendix 1;  |
| "**Data Protection Impact Assessment"** | means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data which includes as a minimum:a systematic description of the envisaged Processing and the purposes of the Processing, including, where applicable, the legitimate interest for which the Processing is carried out;an assessment of the necessity and proportionality of the Processing operations in relation to the purposes pursued;an assessment of the risks to the rights and freedoms of Data Subjects; andthe measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the Data Protection Laws; |
| **"Data Protection Laws"** | means:any Applicable Law to which a Party is subject from time to time in any territory in which they Process Personal Data and which relates to the protection of individuals with regards to the Processing of Personal Data and privacy rights, including without limitation the GDPR (General Data Protection) and the e-Privacy Directive and relevant member state laws in the European Economic Area ("**EEA**") and in relation to the United Kingdom ("**UK**") the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (amended by SI 2011 no. 6) and the GDPR (as incorporated into UK law under the UK European Union (Withdrawal) Act 2018) as the same are amended in accordance with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by SI 2020 no. 1586), as amended to be referred to as **PECR**, **DPA 2018** and the **UK GDPR** respectively, as the same are amended, consolidated, modified, re-enacted or replaced from time to time;any code of practice or guidance published by a Regulator from time to time; and/or any binding pronouncements (including findings, orders, decisions and/or judgements) issued by a Regulator or a court; |
| **"Data Subject"**  | means an identified or identifiable natural person to whom Personal Data relates, regardless of whether the person can be identified directly or indirectly; |
| **"Data Subject Request"** | * + - 1. means an actual or purported request or notice or complaint from or on behalf of a Data Subject exercising his/her rights under the Data Protection Laws including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object;
 |
| **"Data Transfer Agreement"**  | means as applicable:the standard contractual clauses approved by the European Commission for the transfer of Personal Data to third countries issued by the European Commission Decision of 4 June 2021, as amended, varied, supplemented or substituted from time to time, as applicable in respect of transfers of Personal Data from Controllers or Processors in the EEA to Controllers or Processors in Restricted Countries; the addendum approved by the UK Information Commissioner’s Office as amended, varied, supplemented or substituted from time to time;the standard contractual clauses adopted by the government of the United Kingdom, or approved by the government of the United Kingdom as updated, replaced, consolidated and/or amended from time to time, for transfers of Personal Data from Controllers or Processors in the UK to Controllers or Processors in Restricted Countries; orany standard contractual clauses adopted under the Applicable Laws to which a Data Exporter is subject, as updated, replaced, consolidated and/or amended from time to time, for transfers of Personal Data from a Data Exporter to Controllers or Processors in Restricted Countries; |
| **"GDPR"** | * + - 1. means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
 |
| **"Government Access"** | * + - 1. means:

a request for disclosure of Shared Data (which has been transferred in accordance with Paragraph 2.5) by a public authority under the laws of the country of destination; orwhere the Data Importer is aware of direct access to Shared Data (which has been transferred in accordance with Paragraph 2.5) by a public authority under the laws of the country of destination; |
| "**Group**" | means in respect of either Party, that Party, its holding company, its subsidiaries and any other direct or indirect holding company or subsidiary from time to time of such holding company or subsidiary; |
| **"Joint Controllers"** | means where two or more Controllers jointly determine the purposes and means of processing of Personal Data; |
| **"Losses"** | * + - 1. means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
 |
| **"Permitted Recipients"** | * + - 1. means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Appendix 1*;*
 |
| **"Personal Data"** |  means any information relating to a Data Subject, including but not limited to any Special Category Personal Data and data relating to criminal convictions and offences; |
| **"Personal Data Breach"** |  means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed and, for the avoidance of doubt, includes a breach of Paragraph 2.4.2(h); |
| **"Personnel"** | means all persons engaged or employed from time to time by the Associate in connection with this Agreement, including employees, consultants, contractors and permitted agents from time to time; |
| **"Process"** | means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (and "**Processing**" and "**Processed**" shall be construed accordingly); |
| **"Processor"** | means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller; |
| **"Regulator"** | means any local or national agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering, providing guidance on, supervising and enforcing Data Protection Laws, including in the United Kingdom the Information Commissioner's Office, or any successor or replacement body from time to time; |
| **"Regulator Correspondence"** | means any correspondence or communication (whether written or verbal) from a Regulator in relation to the Processing of Personal Data; |
| **"Restricted Country"** | means a country, territory or jurisdiction which: (i) is not covered by an adequacy determination by a competent authority with jurisdiction over the Data Exporter; (ii) or otherwise in relation to which a transfer restriction applies under the Applicable Laws of the Data Exporter; |
| "**Restricted Transfer**" | means:a transfer of Shared Data to a Restricted Country; or an onward transfer from a Data Importer to a third party, in each case where such transfer would be prohibited by Data Protection Laws of the Data Exporter in the absence of a legal transfer mechanism permitted by the Data Protection Laws; |
| **"Security Requirements"** | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws including, in particular:a requirement to only Process Personal Data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;a requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The appropriate level of security shall be assessed by taking into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed;  |
| **"Services"** | means the Services as set out in the Agreement; |
| **"Shared Data"** | means the Personal Data shared between the Parties under, or in connection with, this Agreement (such Personal Data is more particularly described in Appendix 1 (*Data Processing Particulars*)); |
| "Special Category Personal Data”  | means information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation; |
| "**Sub-Processor**" | means any third party Processor appointed by the Associate (including a sub-contractor or any Group company or affiliate, or any Data Importer) to Process the Shared Data on its behalf in connection with the Services (including any sub-Processors of such Sub-Processor) and "**Sub-Processing**" relates to Processing carried out by a Sub-Processor; and |
| "**Third Party Request**" | means a written request from any third party for disclosure of (or access to) Shared Data, including a Data Subject Request (or purported Data Subject Request), a request to rectify, block or erase any Personal Data, any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation, a Government Access request or otherwise, where compliance with such request is required or purported to be required by Applicable Law.  |

**DATA PROTECTION**

Arrangement Between the Parties

* + 1. The Parties each acknowledge and agree that the factual arrangements between them dictate the classification and role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:

the Parties shall each Process the Shared Data;

each Party shall act as a Controller in respect of the Processing of the Shared Data on its own behalf and in particular each shall be a Controller of the Shared Data acting individually and in common, as follows:

the University shall be a Controller where it is Processing the Shared Data in relation to Higher Education (to enable the institution to register students at Kingston University and for Kingston University to provide services under the contract, e.g. Award), and

the Associate shall be a Controller where it is Processing the Shared Data in relation to Higher Education (e.g. in order to manage the student relationship with the Associate)**.**

[each Party shall act as a Controller in respect of the Processing of the Shared Data as Joint Controllers in relation to [insert purpose];] ***[Guidance Note: Only include if the parties will act as joint controllers and if*** ***so insert purpose for which they will be processing the Shared Data as joint controllers.]***

* + 1. Notwithstanding Paragraph 2.1.1(b), if either Party is deemed to be a Joint Controller with the other in relation to the Shared Data, the Parties agree that they shall:

be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations set out in Paragraph 2.4.2(h) where Shared Data has been transmitted by it, or while Shared Data is in its possession or control; and

acting reasonably and in good faith seek by way of variation or additional agreement or arrangement, to document the parties' respective obligations in accordance with Data Protection Laws (particularly in respect of communications with Data Subjects, third parties and a Regulator, including in respect of transparency requirements and notification obligations).

* 1. Each of the Parties acknowledges and agrees that Appendix 1 to this Agreement is an accurate description of the Data Processing Particulars.

Contact Data

* + 1. Notwithstanding Paragraph 2.1 the Parties each acknowledge and agree that they may need to Process Personal Data in relation to each Party's representatives (in their respective capacities as Controllers) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Agreement and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with their respective regulatory obligations.
		2. Each Party shall Process such Personal Data for the purposes set out in Paragraph 2.3.1 in accordance with their respective privacy policies. The Parties acknowledge that they may be required to share Personal Data with members of their Group and other relevant parties, within or outside of the country of origin, in order to carry out the activities listed in Paragraph 2.3.1, and in doing so each Party will ensure that the sharing and use of this Personal Data complies with applicable Data Protection Laws.

Data Controller Obligations

* + 1. Each Party shall in relation to the Processing of the Shared Data comply at all times with its respective obligations under the Data Protection Laws.
		2. Without limiting the generality of the obligation set out in Paragraph 2.4.1, in particular, each Party shall:
			1. only Process the Shared Data for the purposes of providing the Services or taking the benefit of the Services (as applicable) or otherwise in accordance with the terms of this Agreement;]
			2. where required to do so make due notification and make all payments due (as applicable) to the Regulator;
			3. ensure it is not subject to any prohibition or restriction which would:

prevent or restrict it from disclosing or transferring the Shared Data to the other Party as required under this Agreement;

prevent or restrict it from granting the other Party access to the Shared Data as required under this Agreement; or

prevent or restrict either Party from Processing the Shared Data, as envisaged under this Agreement;

* + - 1. ensure that all fair Processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Shared Data as required in order to obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws.
			2. maintain complete and accurate records and information to demonstrate its compliance with this Paragraph 2.4 (Data Controller Obligations);
			3. work together (acting reasonably and in good faith) in the preparation of any Data Protection Impact Assessment (where applicable) prior to commencing any Processing and continue to review the requirement for any Data Protection Impact Assessments should there be a change in the intended purpose for the Processing of the Personal Data;
			4. ensure that the Shared Data disclosed or transferred to, or accessed by, the other Party is accurate and up-to-date, as well as adequate, relevant and not excessive to enable the other Party to Process such Shared Data as envisaged under this Agreement;
			5. ensure that appropriate technical and organisational security measures are in place sufficient to comply with at least the obligations imposed on the Controller by the Security Requirements and at any time where requested provide to the other Party evidence of its compliance.
			6. notify the other Party promptly, and in any event within 24 hours of receipt of any Third Party Requestor Regulator Correspondence which relates directly or indirectly to the Processing of the Shared Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Third Party Request or Regulator Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 2.4.2(i), each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Third Party Request or Regulator Correspondence. [Where acting as a Joint Controller, the Party who has provided the notice (and/or as applicable obtained the necessary consent(s)) pursuant to Paragraph 2.4.2(d) shall be responsible for responding to a Third Party Request or Regulator correspondence and the other Party shall provide all such reasonable assistance as may be required];
			7. use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Shared Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
			8. notify the other Party in writing without undue delay (and in any event within 24 hours upon becoming aware of any actual or suspected or threatened Personal Data Breach in relation to the Shared Data ("Data Loss Event") and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):
				1. seek to recover the compromised data as soon as practicable and implement any measures necessary to restore the security of the compromised Shared Data;
				2. promptly provide the other Party with a report containing details about the nature of the Data Loss Event and provide the other Party with further information in phases, as details become available;
				3. investigate the incident and its cause;
				4. support the other Party to make any required notifications to the Regulator and/or other relevant regulatory body and affected Data Subjects. Where acting as a Joint Controller;

the Party who has suffered the actual or suspected Data Loss Event shall be responsible (with the support of the other joint Controller(s)) for making any required notification to a Regulator; and

the Party who has provided the notice (and/or as applicable obtained the necessary consent(s)) pursuant to Paragraph 2.4.2(d) shall be responsible (with the support of the other joint Controller(s)) for making any required notification to affected Data Subjects; and

* + - * 1. co-ordinate with the other Party the management of public relations and public statements relating to the incident. For the avoidance of doubt the Associate shall make no public statement in relation to the incident without the prior written approval of the University.
			1. take reasonable steps to ensure the reliability of and adequate training of any of its Personnel who have access to the Shared Data;
			2. not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
			3. not transfer any Shared Data it is processing to a Restricted Country except in accordance with Paragraph 3;
			4. hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data;
			5. except to the extent required by Applicable Law, upon the earlier of:
				1. termination or expiry of this Agreement; and/ or
				2. the date on which the Shared Data is no longer relevant to, or necessary for, the provision of the Services,

cease Processing all Shared Data received from the Data Originator and return and/ or permanently and securely destroy such Shared Data and all copies in its possession or control (such that the Shared Data is no longer retrievable), as directed in writing by the Data Originator.

* 1. Each Party will transfer Shared Data to the other in a format agreed between the Parties, which shall apply to each and every occasion that Shared Data is transferred between the Parties, unless agreed otherwise between the Parties.
	2. Where acting as a Controller or Joint Controller, before further sharing the Shared Data with a:
		1. third party where such party shall act as a Controller, the Associate must obtain the consent of the University and enter into an appropriate data sharing agreement with the third party and ensure such third party meets the requirements of the Data Protection Laws and only uses the Shared Data for the purposes permitted and set out in this Agreement.
	3. Except as otherwise provided, this Agreement does not transfer ownership of, or create any licences (implied or otherwise), in any intellectual property rights in any Personal Data.

INTERNATIONAL TRANSFERS

* 1. The Parties acknowledge that to the extent that the University transfers Personal Data to the Associate under this Agreement, it shall be transferring Personal Data to a Restricted Country. In respect of such transfer the Parties shall enter into a Data Transfer Agreement as set out at Appendix 3 on the date of this Agreement and such Data Transfer Agreement shall be incorporated into and form part of this Agreement.
	2. Nothing in this Agreement is intended to undermine or conflict with any terms of the Data Transfer Agreement. In the event of any conflict, the terms of the Data Transfer Agreement shall prevail.

 Third Party Requests

* + 1. Where the Associate, in each case who receive the Shared Data as part of a Restricted Transfer, or any other third party recipients of the Shared Data receive a Third Party Request or becomes aware of Government Access in relation to the Shared Data transferred to it (the “Receiving Party”), the Associate shall, unless prohibited by Applicable Law from doing so, promptly (and in any event within forty-eight (48) hours) notify the University and provide all information available to it (including in the case of a Third Party Request, the requesting authority, legal basis for the request and any initial response provided).
		2. Where the Receiving Party is prohibited by Applicable Law from notifying the University of a Third Party Request or Government Access, it shall use its best efforts to obtain a waiver of the prohibition to notify the University and communicate to any entity requesting such disclosure the following message: “The information you wish to access is the legal responsibility of Kingston University (“the Controller”). The Controller requests in the strongest terms that, before any further steps are taken, you consult the Controller urgently by contacting the Controller’s Data Protection Officer".
		3. In the event of a request or access referred to above, the Receiving Party shall:
			1. review the legality of the request and exhaust all remedies to challenge the request if it concludes there are grounds under the Applicable Laws of the country of receipt to do so. No disclosure shall be made until required under applicable procedural rules;
			2. document its assessment and challenge of the request for disclosure and to the extent permitted under the Applicable Laws of the Data Importer make this available to the University and a Regulator promptly upon request from the University; and
			3. only provide the minimum amount of information possible, based on a reasonable interpretation of the request, including, without limitation, redacting any of the University’s confidential information and Shared Data which is not necessary for the purposes of the request.
	1. In any event, if the request is made to a Data Importer, which as a result of the Third Party Request is no longer able to comply with the Data Transfer Agreement, the Associate shall notify the University of such inability.
	2. The Associate shall ensure the obligations set out in this Paragraph 3 are included within the applicable data processing or sharing agreements it has with any other Receiving Party.
	3. Where the Associate reasonably believes it is obliged under Applicable Law or a Data Transfer Agreement to notify a Regulator or Data Subjects of any Third Party Request or any other compliance breach under Data Protection Laws, the Associate shall seek the consent of the University (which shall not be unreasonably withheld).]

**Recoverable Loss AND COMPENSATION**

* 1. Nothing in this Agreement shall prevent the University from recovering any Losses it incurs in relation to:
		1. legal fees, on a solicitor/client basis;
		2. other professional charges and expenses;
		3. disbursements;
		4. costs of investigation including forensic investigation;
		5. cost of breach notification, including notifications to Data Subjects, Regulator(s) or any other parties including listing authorities whether notification is required under Applicable Law or otherwise made in the reasonable belief that notification is necessary;
		6. cost of complaints handling, including providing Data Subjects with credit and/or fraud monitoring services and/or credit reference checks, setting up contact centres (e.g. call centres), and making ex gratia payments;
		7. costs of claims;
		8. cost of litigation;
		9. costs of settlement, including ex gratia payments;
		10. judgment interest; and
		11. penalties, including fines.
	2. To the extent that the Associate has an entitlement under Data Protection Laws to claim from the University compensation paid by the Associate to a Data Subject or third party as a result of a breach of Data Protection Laws (in full or in part) by the University, the University shall be liable only for such amount as directly relates to the University’s responsibility for any damage caused to the relevant Data Subject or third party. For the avoidance of doubt the University shall only be liable to make payment to the Associate under this Paragraph 4.2, upon receipt of evidence from the Associate, which shall be to the University’s reasonable satisfaction and that clearly demonstrates:
		1. that the University has breached Data Protection Laws;
		2. that such breach contributed (in part or in full) to the harm caused entitling the relevant Data Subject or third party to receive compensation in accordance with Data Protection Laws; and
	3. the proportion of responsibility for the harm caused to the relevant Data Subject or third party which is attributable to the University.

INDEMNITY

* 1. Both Parties shall indemnify on demand and keep indemnified and held harmless the other Party from and against all and any Losses that are sustained, suffered or incurred by, awarded against or agreed to be paid by the other Party to the extent arising from the first Party's breach of its obligations under this Schedule and/or failure to comply with the Data Protection Laws, including, in particular all Losses resulting from:
		1. any monetary penalties or fines levied by any Regulator on the other Party;
		2. the costs of any investigative, corrective or compensatory action required by a Regulator, or of defending any proposed or actual enforcement taken by a Regulator including if such investigation arises as a result of a self-report or otherwise;
		3. any Losses suffered or incurred by, awarded against, or agreed to be paid by the other Party pursuant to a claim, action or challenge made by a third party to or against the other Party (including by (or on behalf of) a Data Subject); and
		4. except to the extent covered by Paragraphs 6.1.1 and/ or 6.1.2 and/ or 6.1.3, any Losses suffered or incurred, awarded against or agreed to be paid by the other Party.]

INSURANCE

* 1. Both Parties agree:
		1. to obtain and keep in full force and effect at all times, in respect of the Processing of the Personal Data, a policy or policies of insurance covering liability for damage arising to persons as a result of the Party's breach of this Schedule **5c** (Data Protection) and/or failure to comply with the Data Protection Laws and which meet the following conditions:
			1. it must cover liability for damage arising to any person;
			2. it must apply in relation to the Processing of Personal Data;

**AUDIT**

The Associate shall within 30 calendar days of a request from the University, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the University (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Schedule.

**termination**

* 1. Notwithstanding anything in this Agreement to the contrary, this Schedule shall continue in full force and effect for so long as either Party Processes any Shared Data received from the other Party.
	2. In the case of any non-compliance by the Associate with any of the obligations under this Agreement, the Data Protection Laws, the University may, by giving written notice unilaterally:
		1. immediately terminate this Agreement; and/or
		2. suspend any data submission under this Agreement; and/or
		3. require the Associate to cease or suspend any Processing of Shared Data including in specific locations.

GOVERNING LAW

This Schedule **5c** shall be governed by and construed in accordance with English Law.

Appendix 1

Data Protection Particulars

|  |  |
| --- | --- |
| **The subject matter and duration of the Processing** | The subject matter as defined in the Agreement for the duration of the Agreement |
| **The nature and purpose of the Processing** | Higher Education to enable the institution to register students at Kingston University and for Kingston University to provide services under the contract, e.g. Award.  |
| **The type of Personal Data being Processed** | Highlight relevant Personal Data:NameDate of birthAddressNationalityNext of kinStudent recordsStaff info relevant to service deliveryOther: Other information the parties are required to hold as part of their statutory reporting duties.Highlight relevant Special Category Personal Data/criminal convictions:Data/criminal convictions: Race or ethnic origin ~~Political opinions~~ ~~Religious or philosophical beliefs~~ ~~Trade union membership~~ ~~Genetic data~~ ~~Biometrics~~ Physical or mental health ~~Sex life or sexual orientation~~ Criminal convictions and offences  |
| **The categories of Data Subjects** | Highlight categories below:StudentsStaffOther N/A |
| **Data Retention/Deletion Period and Process** | In line with Kingston University Retention Policy.  |
| **Locations (including the geographic region) in which the personal data may be Processed by the Associate** | Kingston University, Holmwood House, Grove Crescent, Kingston upon Thames, Surrey KT1 2EE, United Kingdom [insert Associate name and location] |

Page 23 of 23

**Appendix 2**

**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.

**\*\*KU explanatory note**:

Please complete Parts 1, 2 and 3 with details specific to your agreement.

In Part 1 Tables 2 and 3, the Data Protection Team have indicated the default answers expected to be appropriate in most cases, by striking through the other answers.

If you need advice on Part 1, Table 4 please contact it-security@kingston.ac.uk. If you have any other queries, please contact dataprotection@kingston.ac.uk.

Please delete this explanatory note before finalising the agreement.\*\*

## 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: Kingston University Higher Education CorporationTrading name (if different): Kingston UniversityMain address (if a company registered address): Holmwood House, Grove Crescent, Kingston upon Thames, Surrey, KT1 2EE, United KingdomOfficial registration number (if any) (company number or similar identifier): Charity number: X12530 | Full legal name: [insert details here]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): [insert details of Head of QAE (Quality Assurance & Enhancement)]Job Title:      Contact details including email:       | Full Name (optional): [insert details here]     Job Title:      Contact details including email:       |
| **Importer Data Subject Contact** |  | Job Title: [insert details here]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 aboveSigned: [insert details of VC (Vice Chancellor) here]→ Date of signature: xx/xx/20xxFull name:      Job title:       | Signed for and on behalf of the **Importer** set out aboveSigned: [insert details here]→ Date of signature: xx/xx/20xxFull name:      Job title:       |

### Table 2: Transfer Details

|  |  |
| --- | --- |
| **UK country’s law that governs the IDTA:** | England and Wales |
| **Primary place for legal claims to be made by the Parties** | England and Wales |
| **The status of the Exporter** | In relation to the Processing of the Transferred Data:Exporter is a Controller |
| **The status of the Importer** | In relation to the Processing of the Transferred Data:Importer is a Controller |
| **Whether UK GDPR applies to the Importer** | UK GDPR applies to the Importer’s Processing of the Transferred Data |
| **Linked Agreement** | **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: [insert details here] Institutional Agreement between Kingston University and xyzDate of agreement:      Parties to the agreement:      Reference (if any): Institutional Agreement |
|  **Term** | The Importer may Process the Transferred Data for the following time period: the period for which the Linked Agreement is in force |
| **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. |
| **Ending the IDTA when the Approved IDTA changes** | Which Parties may end the IDTA as set out in Section ‎29.2:ImporterExporter |
| **Can the Importer make further transfers of 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. |
| **Review Dates**  | 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.  |
| **Special Categories of Personal Data and criminal convictions and offences** | The Transferred Data includes data relating to:racial or ethnic originpolitical opinionsreligious or philosophical beliefstrade union membershipgenetic databiometric data for the purpose of uniquely identifying a natural personphysical or mental health sex life or sexual orientationcriminal convictions and offencesnone of the aboveset 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.  |
| **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.  |
| **Purpose** | The Importer may Process the Transferred Data for the purposes set out in: Appendix 1, Data Protection Particulars.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.  |

### Table 4: Security Requirements

|  |  |
| --- | --- |
| **Security of Transmission** | Data will be shared via SharePoint with the Kingston University logins (kpxxxxx) allocated to the relevant Associate Staff members. As an alternative, data may be shared via SharePoint with named external email addresses. Shared files will be protected by password.  |
| **Security of Storage** | N/A |
| **Security of Processing** | N/A |
| **Organisational security measures** | N/A |
| **Technical security minimum requirements** | N/A |
| **Updates to the Security Requirements** | The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.  |

##

## Part 2: Extra Protection Clauses

|  |  |
| --- | --- |
| **Extra Protection Clauses:** | N/A |
| **(i) Extra technical security protections** | N/A |
| **(ii) Extra organisational protections** | N/A |
| **(iii) Extra contractual protections** | N/A |

##

## Part 3: Commercial Clauses

|  |  |
| --- | --- |
| **Commercial Clauses** | N/A |

## Part 4: Mandatory Clauses

### Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements
	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.
	2. This IDTA is made up of:
		1. Part one: Tables;
		2. Part two: Extra Protection Clauses;
		3. Part three: Commercial Clauses; and
		4. Part four: Mandatory Clauses.
	3. The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
	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).
	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
	1. If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
	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
	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.
	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:
		1. the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
		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. 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
	1. The Parties may choose to each sign (or execute):
		1. the same copy of this IDTA;
		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;
		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.

1. Changing this IDTA
	1. Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
		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;
		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;
		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
		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.

* 1. 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.
	2. 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.
	3. From time to time, the ICO (Information Commissioner s Office) may publish a revised Approved IDTA which:
		1. makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or
		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.

1. Understanding this IDTA
	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.
	2. If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
	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.
	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.
	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. 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.
	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):
		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
		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.
	8. The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
	9. References to:
		1. singular or plural words or people, also includes the plural or singular of those words or people;
		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
		3. any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.
2. Which laws apply to this IDTA
	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

1. The Appropriate Safeguards
	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:
		1. both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
		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.
	2. The Exporter must:
		1. ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
		2. (if the Importer reasonably requests) provide it with a copy of any TRA.
	3. The Importer must:
		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”);
		2. co-operate with the Exporter to ensure compliance with the Exporter’s obligations under the UK Data Protection Laws;
		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
		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.
	4. The Importer must ensure that at the Start Date and during the Term:
		1. the Importer Information is accurate;
		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.
	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.
2. Reviews to ensure the Appropriate Safeguards continue
	1. Each Party must:
		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
		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.
	2. If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
		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;
		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
		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.
3. The ICO
	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.
	2. The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
	3. The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

### The Exporter

1. Exporter’s obligations
	1. The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
	2. The Exporter must:
		1. comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
		2. comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
		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.
	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.
	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.
	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

1. General Importer obligations
	1. The Importer must:
		1. only Process the Transferred Data for the Purpose;
		2. comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
		3. comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
		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;
		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
		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).
	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.
2. Importer’s obligations if it is subject to the UK Data Protection Laws
	1. If the Importer’s Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:
		1. UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
		2. it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.
	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).
1. Importer’s obligations to comply with key data protection principles
	1. The Importer does not need to comply with this Section 14 if it is the Exporter’s Processor or Sub-Processor.
	2. The Importer must:
		1. ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
		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
		3. ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
2. What happens if there is an Importer Personal Data Breach
	1. If there is an Importer Personal Data Breach, the Importer must:
		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
		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.
	2. If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
		1. notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
			1. a description of the nature of the Importer Personal Data Breach;
			2. (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
			3. likely consequences of the Importer Personal Data Breach;
			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;
			5. contact point for more information; and
			6. any other information reasonably requested by the Exporter,
		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
		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.
	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:
		1. a description of the nature of the Importer Personal Data Breach;
		2. (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
		3. likely consequences of the Importer Personal Data Breach;
		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;
		5. contact point for more information; and
		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.

* 1. 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.
	2. 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.

1. Transferring on the Transferred Data
	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:
		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
		2. the third party has been added to this IDTA as a Party; or
		3. if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
		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
		5. the transfer is to the UK or an Adequate Country.
	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).
2. Importer’s responsibility if it authorises others to perform its obligations
	1. The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
	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.
	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.
	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?

1. The right to a copy of the IDTA
	1. If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
		1. it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
		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;
		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.
2. The right to Information about the Importer and its Processing
	1. The Importer does not need to comply with this Section 19 if it is the Exporter’s Processor or Sub-Processor.
	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.

* 1. 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.
	2. 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.
1. How Relevant Data Subjects can exercise their data subject rights
	1. The Importer does not need to comply with this Section 20 if it is the Exporter’s Processor or Sub-Processor.
	2. If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.
	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.
	4. If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:
		1. Without Undue Delay (and in any event within one month);
		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;
		3. in clear and plain English that is easy to understand; and
		4. in an easily accessible form

together with

* + 1. (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
		2. information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
	1. If a Relevant Data Subject requests, the Importer must:
		1. rectify inaccurate or incomplete Transferred Data;
		2. erase Transferred Data if it is being Processed in breach of this IDTA;
		3. cease using it for direct marketing purposes; and
		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.
	2. 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:
		1. the Relevant Data Subject has given their explicit consent to such Decision-Making; or
		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
		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.
1. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor
	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.
2. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws
	1. The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
		1. it is unable to reasonably verify the identity of an individual making the request; or
		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
		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

1. Access requests and direct access
	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.
	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.
	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.
	4. In so far as Local Laws allow, the Importer must:
		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
		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.
2. Giving notice
	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.
	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 bounce back is received.
	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.
3. General clauses
	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:
		1. contain all the terms and conditions agreed by the Parties; and
		2. override all previous contacts and arrangements, whether oral or in writing.
	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.
	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.
	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.
	5. This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
	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.
	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.
	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:
		1. it only applies in so far as it explicitly waives specific rights or remedies;
		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
		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?

1. Breaches of this IDTA
	1. Each Party must notify the other Party in writing (and with all relevant details) if it:
		1. has breached this IDTA; or
		2. it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
	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.
2. Breaches of this IDTA by the Importer
	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.
	2. Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
		1. the Exporter must suspend sending Transferred Data to the Importer;
		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
		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:
			1. notify the third party receiver of the breach and suspend sending it Transferred Data; and
			2. 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).
	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.
3. Breaches of this IDTA by the Exporter
	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.
	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.
	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

1. How to end this IDTA without there being a breach
	1. The IDTA will end:
		1. at the end of the Term stated in Table 2: Transfer Details; or
		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;
		3. at any time that the Parties agree in writing that it will end; or
		4. at the time set out in Section ‎29.2.
	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:
		1. its direct costs of performing its obligations under the IDTA; and/or
		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.

1. How to end this IDTA if there is a breach
	1. A Party may end this IDTA immediately by giving the other Party written notice if:
		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
			1. 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
			2. the breach and its Significant Harmful Impact cannot be corrected;
		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.
2. What must the Parties do when the IDTA ends?
	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:
		1. notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;
		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
		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.
	2. When this IDTA ends (no matter what the reason is):
		1. the Exporter must stop sending Transferred Data to the Importer; and
		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;
		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.
		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

1. Your liability
	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.
	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:
		1. Party One’s breach of this IDTA; and/or
		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;
		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.

* 1. 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.
	2. 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.
1. How Relevant Data Subjects and the ICO may bring legal claims
	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.
	1. 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).
	2. 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).
	3. 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.
	4. 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.
1. Courts legal claims can be brought in
	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).
	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.
	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
	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.
	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).
2. Arbitration
	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.
	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.
	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.
	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.
	5. The English language must be used in the arbitral proceedings.
	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.
3. 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. |
| 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 8.3.1, 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. 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-ProcessorIf 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. |