Joint Schedule 10 (Processing Data)

[Category Guidance: it is critical that you liaise with the CCS Data Protection Officer to discuss the data processing activities of your commercial agreement. A copy of this Schedule's Annex 1 should be completed for your commercial agreement to reflect the data processing occurring at commercial agreement level. Buyers will need to complete their own version of this form to reflect the data processing activities for their individual call-offs. Category must delete this guidance once complete.]

[Buyer Guidance: the Buyer will be the Controller, and the Supplier the Processor in the vast majority of cases. If the Buyer believes another data processing scenario applies, such as the Parties being Joint or Independent Controllers, the Buyer must speak to its data protection team or Data Protection Officer. Making the Supplier a Controller over Buyer information can create risks for the Buyer, and the Buyer must make sure it understands the consequences of this.]

1. Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 *(Definitions)*:

"Independent Controller"	a party which is a Controller of the same Personal Data as the other Party and there is an element of joint control with regards to that Personal Data;
"Joint Control"	where two (2) or more Controllers jointly determine the purposes and means of Processing;
"Joint Controllers"	has the meaning given in Article 26 of the UK GDPR, or EU GDPR, as the context requires; and
"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract.

2. Status of the Controller

2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

2.1.1 "Controller" in respect of the other Party who is "Processor";

2.1.2 "Processor" in respect of the other Party who is "Controller";

2.1.3 "Joint Controller" with the other Party;

2.1.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

3. Where one Party is Controller and the other Party its Processor

3.1 Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller or further provided in writing by the Controller and may not be determined by the Processor.

3.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

3.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

3.3.1 a systematic description of the envisaged Processing and the purpose of the Processing;

3.3.2 an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

3.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

3.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data; and

3.3.5 providing assurance that the measures referred to in Paragraph 3.3.4 comply with the Security Requirements (if any).

3.4 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

3.4.1 process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*) or as further provided in writing by the Controller, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

3.4.2 ensure that it has in place Protective Measures including in the case of the Supplier the measures set out in this Joint Schedule 10 *(Processing Data)*, Clause 17.3 of the General Terms and the Security Requirements (if any), which the Controller may reasonably reject (including, where applicable in accordance with its rights of rejection under those provisions) but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures.

3.4.3 ensure that:

(a) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*)) and the Controller's further written instructions;

(b) it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are subject to any staff vetting required by this Contract, including the Security Requirements (if any);

(ii) are aware of and comply with the Processor's duties under this Joint Schedule 10, the Security Requirements (if any) and Clauses 17 (*Data protection*), 18 (*What you must keep confidential*) and 19 (*When you can share information*) of the General Terms;

(iii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(iv) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(v) have undergone adequate training in the use, care, protection and handling of Personal Data (including any training required by the Security Requirements (if any));

3.4.4 not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(a) the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74 of the DPA 2018) and/or Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(i) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying

on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(ii) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 3.4.4(a); and

(iii) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(A) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 3.4.4(a);

(B) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 3.4.4(a); and/or

(C) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 3.4.4(a)(ii) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

(b) the Controller and/or the Processor have provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:

(i) where the transfer is subject to UK GDPR;

(A) the International Data Transfer Agreement (“issued by the Information

Commissioner under s119A(1) of the DPA 2018 (the "**IDTA**"); or

(B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("**EU SCCs**") together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018; and/or

(ii) where the transfer is subject to EU GDPR, the EU SCCs,

as well as any additional measures being determined by the Controller being implemented by the importing party;

(c) the Data Subject has enforceable rights and effective legal remedies;

(d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

3.4.5 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

3.5 Subject to Paragraph 3.6 of this Joint Schedule 10, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

3.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

3.5.2 receives a request to rectify, block or erase any Personal Data;

3.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

3.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

3.5.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

3.5.6 becomes aware of a Data Loss Event.

3.6 The Processor's obligation to notify under Paragraph 3.5 of this Joint Schedule 10 shall include the provision of further information to the Controller, as details become available.

3.7 Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 3.5 of this Joint Schedule 10 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

3.7.1 the Controller with full details and copies of the complaint, communication or request;

3.7.2 such assistance as is reasonably requested by the Controller to enable the it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

3.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

3.7.4 assistance as requested by the Controller following any Data Loss Event; and/or

3.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

3.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 10. This requirement does not apply where the Processor employs fewer than two hundred and fifty (250) staff, unless:

3.8.1 the Controller determines that the Processing is not occasional;

3.8.2 the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

3.8.3 the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

3.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

3.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

3.11 Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

3.11.1 notify the Controller in writing of the intended Subprocessor and Processing;

3.11.2 obtain the written consent of the Controller;

3.11.3 enter into a written agreement with the Subprocessor which gives effect to the terms set out in this Joint Schedule 10 such that they apply to the Subprocessor; and

3.11.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

3.12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

3.13 The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 10 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

3.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office, any relevant Central Government Body and/or any other regulatory authority. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office, relevant Central Government Body and/or any other regulatory authority.

4. Where the Parties are Joint Controllers of Personal Data

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 (Joint Controllers Agreement) to this Joint Schedule 10.

5. Independent Controllers of Personal Data

5.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

5.2 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

5.3 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 5.2 of this Joint Schedule 10 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

5.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

5.5 The Parties shall only provide Personal Data to each other:

5.5.1 to the extent necessary to perform their respective obligations under the Contract;

5.5.2 in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects:

(a) where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK and/or the EEA, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(A) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(B) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer

mechanisms in compliance with this Paragraph 5.5.2(a)(i); and

(C) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(1) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 5.5.2(a)(i);

(2) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 5.5.2(a)(i); and/or

(3) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 5.5.2(a)(i)(B) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

(b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable)) as determined by the non-transferring Party which could include:

(i) where the transfer is subject to UK GDPR:

(A) the International Data Transfer Agreement (the "**IDTA**") ""as published by the Information Commissioner's Office or such updated version of such IDTA as is published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time; or

(B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European

Commission from time to time (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(ii) where the transfer is subject to EU GDPR, the EU SCCs,

as well as any additional measures determined by the Controller being implemented by the importing party;

(c) the Data Subject has enforceable rights and effective legal remedies;

(d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

4.5.4 where it has recorded it in Annex 1 *(Processing Personal Data).*

5.6 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, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

5.7 A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

5.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

5.8.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

5.8.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(a) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(b) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

5.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:

5.9.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

5.9.2 implement any measures necessary to restore the security of any compromised Personal Data;

5.9.3 work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

5.9.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

5.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

5.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

5.12 Notwithstanding the general application of Paragraphs 3.1 to 3.14 of this Joint Schedule 10 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 5.2 to 5.12 of this Joint Schedule 10.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: **[Insert** Contact details]

1.2 The contact details of the Supplier's Data Protection Officer are: **[Insert** Contact details]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

[Buyer Guidance: the Buyer will be the Controller, and the Supplier the Processor in the vast majority of cases. If you believe another data processing scenario applies, such as the Parties being Joint or Independent Controllers, you must speak to your data protection team or DPO.]

Description	Details
Identity of Controller and Processor for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: ● **[Insert** the scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority] **The Supplier is Controller and the Relevant Authority is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with Paragraph 2 of the following Personal Data: ● **[Insert** the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier] **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:

	• **[Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together] **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* • *Personally identifiable information of Supplier Staff for which the Supplier is the Controller,* • *Personally identifiable information of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Staff) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,* • **[Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority] ***[Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]*
Subject matter of the Processing	**[Insert** This should be a high level, short description of what the processing is about i.e. its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide [insert description of relevant service].]
Duration of the Processing	[**Insert** Clearly set out the duration of the Processing including dates]
Nature and purposes of the Processing	[**Insert** Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the Processing means any operation 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 of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	[**Insert** Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[**Insert** Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	[**Insert** Describe how long the data will be retained for, how it be returned or destroyed]
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	[**Insert** Clearly identify each location, explain where geographically personal data may be stored or accessed from. Explain the legal gateway you are relying on to export the data e.g. adequacy decision, EU SCCs, UK IDTA. Annex any SCCs or IDTA to this contract]]
Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under the Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event (noting	[**Insert** Please be as specific as possible. Any Protective Measures must be in accordance with the Security Requirements.]

that any Protective Measures are to be in accordance with any Security Requirements)	

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of Paragraphs 3 of Joint Schedule 10 (Where one Party is Controller and the other Party is Processor) and Paragraphs 5.2 to 5.12 of Joint Schedule 10 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

1.2.1 is the exclusive point of contact for Data Subjects and is responsible for using best endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

1.2.2 shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and

1.2.5 shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

2.1.1 report to the other Party every [x] months on:

(a) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(b) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(c) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(e) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1(a) to 2.1.1(e);

2.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 2.1.1(c) to (e) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

2.1.5 request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;

2.1.6 ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

2.1.7 use best endeavours to ensure the reliability and integrity of any of its Processor Personnel who have access to the Personal Data and ensure that its Processor Personnel:

(a) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(b) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(c) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

2.1.8 ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

2.1.9 ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

2.1.10 ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.1.11 not transfer such Personal Data outside of the UK and/or the EEA unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(a) the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(i) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and

continue to be self-certified on the US Data Privacy Framework;

(ii) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 2.1.11(a); and

(iii) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(A) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 2.1.11(a);

(B) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 2.1.11(a); and/or

(C) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 2.1.11(a)(ii) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

(b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable) as agreed with the non-transferring Party which could include

(i) where the transfer is subject to UK GDPR, the UK International Data Transfer Agreement (the "**IDTA**") published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time; or

(ii) The European Commission's Standard Contractual Clauses per decision 2021/914/EU or

such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(iii) where the transfer is subject to EU GDPR, the EU SCCs.

as well as any additional measures determined by the Controller being implemented by the importing party;

(c) the Data Subject has enforceable rights and effective legal remedies;

(d) the transferring Party complies with its obligations under Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

2.2 Each Joint Controller shall use its best endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. **Data Protection Breach**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within forty eight (48) hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Personal Data Breach, providing the Buyer and its advisors with:

3.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Eventh under the Data Protection Legislation;

3.1.2 all reasonable assistance, including:

(a) co-operation with the other Party and the Information Commissioner and any other regulatory authority investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(b) co-operation with the other Party including using such best endeavours as are directed by the Buyer to assist in the investigation, mitigation and remediation of a Data Loss Event;

(c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event; and/or

(d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner and/or any other regulatory authority investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Paragraph 3.2.

3.2 Each Party shall use best endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Data Loss Event as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Data Loss Event, including providing the other Party, as soon as possible and within forty eight (48) hours of the Data Loss Event relating to the Data Loss Event, in particular:

3.2.1 the nature of the Data Loss Event;

3.2.2 the nature of Personal Data affected;

3.2.3 the categories and number of Data Subjects concerned;

3.2.4 the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

3.2.5 measures taken or proposed to be taken to address the Data Loss Event; and

3.2.6 describe the likely consequences of the Data Loss Event.

4. **Audit**

4.1 The Supplier shall permit:

4.1.1 the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

4.1.2 the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third

party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

5.1 The Parties shall:

5.1.1 provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

5.1.2 maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority.

7. **Liabilities for Data Protection Breach**

[Buyer Guidance: This Paragraph represents a risk share, the Buyer may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner or any other regulatory authority on either the Relevant Authority or the Supplier for a Data Loss Event ("**Financial Penalties**") then the following shall occur:

7.1.1 if in the view of the Information Commissioner or any other regulatory authority, the Relevant Authority is responsible for the Data Loss Event, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Data Loss Event. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

7.1.2 if in the view of the Information Commissioner or any other regulatory authority, the Supplier is responsible for the Data Loss Event, in that it is not a Data Loss Event that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Data Loss Event; or

7.1.3 if no view as to responsibility is expressed by the Information Commissioner or any other regulatory authority, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 38 *(Resolving disputes)* of the General Terms.

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event shall be liable for the losses arising from such Data Loss Event. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Data Loss Event (the "Claim Losses"):

7.3.1 if the Relevant Authority is responsible for the relevant Data Loss Event, then the Relevant Authority shall be responsible for the Claim Losses;

7.3.2 if the Supplier is responsible for the relevant Data Loss Event, then the Supplier shall be responsible for the Claim Losses: and

7.3.3 if responsibility for the relevant Data Loss Event is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either Paragraph 7.2 or Paragraph 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Data Loss Event, having regard to all the circumstances of the Data Loss Event and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in Material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 13.3 *(When CCS or the Buyer can end a contract)* of the General Terms and the consequences of termination in Clause 13.4.1 of the General Terms shall apply.

9. **Sub-Processing**

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

9.1.1 carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

9.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.