**Joint Schedule 11 (Processing Data)**

**Status of the Controller**

* 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. A Party may act as:
     1. “Controller” in respect of the other Party who is “Processor”;
     2. “Processor” in respect of the other Party who is “Controller”;
     3. “Joint Controller” with the other Party;
     4. “Independent Controller” of the Personal Data where there 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.

**Where one Party is Controller and the other Party its Processor**

* 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.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
  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:
     1. a systematic description of the envisaged Processing and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing in relation to the Services;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
  4. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
     1. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
     2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
        1. nature of the data to be protected;
        2. harm that might result from a Personal Data Breach;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure that :
        1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
        2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
           1. are aware of and comply with the Processor’s duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
           2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
           3. 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
           4. have undergone adequate training in the use, care, protection and handling of Personal Data;
     4. not transfer Personal Data outside of the UK or European Economic Area unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
        1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46) as determined by the Controller;
        2. the Data Subject has enforceable rights and effective legal remedies;
        3. 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
        4. 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
        5. the Controller and the Processor agree that without any further action being required they have entered into the ICO’s Standard Contractual Clauses set out in Annex 4 to this Schedule 11 in respect of the processing of Personal Data outside of the UK and the European Economic Area.
     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.
  5. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
     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
     6. becomes aware of a Personal Data Breach.
  6. The Processor’s obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
  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 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
     1. the Controller with full details and copies of the complaint, communication or request;
     2. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
     3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
     4. assistance as requested by the Controller following any Personal Data Breach; and/or
     5. assistance as requested by the Controller with respect to any request from the Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.
  8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
     1. the Controller determines that the Processing is not occasional;
     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. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
  9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
  10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
  11. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
      1. notify the Controller in writing of the intended Subprocessor and Processing;
      2. obtain the written consent of the Controller;
      3. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
      4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
  12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
  13. UKEF may, at any time on not less than 30 Working Days’ notice, revise this Joint Schedule 11 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).
  14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. UKEF may on not less than 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.

**Where the Parties are Joint Controllers of Personal Data**

* 1. 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 to this Joint Schedule 11 (*Processing Data*).

**Independent Controllers of Personal Data**

* 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.
  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.
  3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 17 of this Joint Schedule 11 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.
  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. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Contract;
     2. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
     3. where it has recorded it in Annex 1 *(Processing Personal Data).*
  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.
  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.
  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”)**:
     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
     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:
        1. 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
        2. 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.
  9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. work with the other Party to make any required notifications to the Information Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
     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.
  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).*
  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)*.
  12. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 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 17 to 27 of this Joint Schedule 11.
  13. In the event that both Parties are Controllers of the Personal Data and for the purposes of the Services the Personal Data will be transferred outside of the UK and the European Economic Area the Parties agree:
  14. that without any further action being required they have entered into the ICO’s Standard Contractual Clauses set out in Annex 3 to this Schedule 11 in respect of data transfers by the Supplier outside of the UK and the European Economic Area;
  15. to use best endeavours to complete the annexes to the Standard Contractual Clauses promptly and at their own cost for the purpose of giving full effect to them; and
  16. that if there is any conflict between the Contract and the Standard Contractual Clauses the terms of the Standard Contractual Clauses shall apply.

## Annex 1 - Processing Personal Data

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

* + - 1. The contact details of UKEF’s Data Protection Officer are: **[Insert** Contact details]
      2. The contact details of the Supplier’s Data Protection Officer are: **[Insert** Contact details]
      3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
      4. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **UKEF is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, UKEF 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 UKEF]*   **The Supplier is Controller and UKEF is Processor**  *The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and UKEF is the Processor in accordance with paragraph* 2 *to paragraph 15* *of the following Personal Data:*   * ***[Insert*** *the scope of Personal Data which the purposes and means of the Processing by UKEF 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:*   * *Business contact details of Supplier Personnel for which the Supplier is the Controller,* * *Business contact details of any* *directors, officers, employees, agents, consultants and contractors of Relevant UKEF (excluding the Supplier Personnel) engaged in the performance of UKEF’s duties under the Contract) for which UKEF 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 UKEF 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 UKEF]*     ***[Guidance*** *where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]* |
| Duration of the Processing | *[Clearly set out the duration of the Processing including dates]* |
| Nature and purposes of the Processing | *[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 | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]* |
| Categories of Data Subject | *[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 Union or Member State law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |

**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 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (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/UKEF]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) 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;

(c) 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;

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

(e) 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/UKEF’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 Clause 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.

* + 1. **Undertakings of both Parties**
       1. The Supplier and UKEF each undertake that they shall:

(a) report to the other Party every [x] months on:

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

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

(iii) 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;

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

(v) 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;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services 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) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. 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;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) 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;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

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

(ii) 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;

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

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) 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 it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable 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 clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing UKEF and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

co-operation with the other Party including taking such reasonable steps as are directed by UKEF to assist in the investigation, mitigation and remediation of a Personal Data Breach;

co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach 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 Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4**. Audit**

4.1 The Supplier shall permit:

1. UKEF, or a third-party auditor acting under UKEF’s direction, to conduct, at UKEF’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
2. UKEF, or a third-party auditor acting under UKEF’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 Services.

4.2 UKEF may, in its sole discretion, require the Supplier to provide evidence of the Supplier’s compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

**5. Impact Assessments**

5.1 The Parties shall:

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
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 and/or any relevant Central Government Body. UKEF 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 and/or any relevant Central Government Body.

**7. Liabilities for Data Protection Breach**

**[Guidance:** This clause represents a risk share, you 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 on either UKEF or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

1. if in the view of the Information Commissioner, UKEF is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of UKEF, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by UKEF, then UKEF shall be responsible for the payment of such Financial Penalties. In this case, UKEF will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to UKEF 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;
2. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that UKEF is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to UKEF and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
3. if no view as to responsibility is expressed by the Information Commissioner, then UKEF 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 34 of the Core Terms (*Resolving disputes*).

## 7.2 If either UKEF 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 Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. 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 Personal Data Breach (the “Claim Losses”):

1. if UKEF is responsible for the relevant Personal Data Breach, then UKEF shall be responsible for the Claim Losses;
2. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
3. if responsibility for the relevant Personal Data Breach is unclear, then UKEF and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude UKEF 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 Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of UKEF.

**8. Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), UKEF shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the Contract*).

**9. Sub-Processing**

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

(a) 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

(b) 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 a 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.

**Annex 3**

**Controller to Controller Standard Contractual Clauses**

**Standard contractual clauses for the transfer of Personal Data from the UK to third countries (Controller to Controller transfers)**

**Data transfer agreement**

between

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(name)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(address and country of establishment)

hereinafter “Data Exporter”)

and

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(address and country of establishment)

hereinafter “Data Importer”

each a “Party”; together “the Parties”.

**Definitions**

For the purposes of the clauses:

1. “Personal Data”, “Special Categories of Data/Sensitive Data”, “Process/Processing”, “Controller”, “Processor”, “Data Subject” and “Commissioner” shall have the same meaning as in the UK GDPR.
2. “the Data Exporter” shall mean the Controller who transfers the Personal Data;
3. “the Data Importer” shall mean the Controller who agrees to receive from the Data Exporter Personal Data for further Processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
4. “clauses” shall mean these standard contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the Parties under the Contract.

The details of the transfer (as well as the Personal Data covered) are specified in Annex B, which forms an integral part of the clauses.

1. **Obligations of the Data Exporter**

The Data Exporter warrants and undertakes that:

1. The Personal Data have been collected, Processed and transferred in accordance with the laws applicable to the Data Exporter.
2. It has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses.
3. It will provide the Data Importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the Data Exporter is established.
4. It will respond to enquiries from Data Subjects and the Commissioner concerning Processing of the Personal Data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.
5. It will make available, upon request, a copy of the clauses to Data Subjects who are third party beneficiaries under clause III, unless the clauses contain Confidential Information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform Data Subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Commissioner. However, the Data Exporter shall abide by a decision of the Commissioner regarding access to the full text of the clauses by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of the clauses to the Commissioner where required.
6. **Obligations of the Data Importer**

The Data Importer warrants and undertakes that:

1. It will have in place appropriate technical and organisational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected.
2. It will have in place procedures so that any third party it authorises to have access to the Personal Data, including Processors, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Importer, including a data Processor, shall be obligated to Process the Personal Data only on instructions from the Data Importer. This provision does not apply to persons authorised or required by Law or regulation to have access to the Personal Data.
3. It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the Data Exporter (which will pass such notification on to the Commissioner where required) if it becomes aware of any such laws.
4. It will Process the Personal Data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
5. It will identify to the Data Exporter a contact point within its organisation authorised to respond to enquiries concerning Processing of the Personal Data, and will cooperate in good faith with the Data Exporter, the Data Subject and the Commissioner concerning all such enquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if the parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of clause I(e).
6. At the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
7. Upon reasonable request of the Data Exporter, it will submit its data Processing facilities, data files and documentation needed for Processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.
8. It will Process the Personal Data, at its option, in accordance with:
9. the data protection laws of the country in which the Data Exporter is established, or

## the relevant provisions[[1]](#footnote-1)of any UK adequacy regulations pursuant to Section 17A Data Protection Act 2018 or Paras 4,5 & 6 Schedule 21 Data Protection Act 2018, where the Data Importer complies with the relevant provisions of such adequacy regulations and is based in a country to which such adequacy regulations pertains, but is not covered by such adequacy regulations for the purposes of the transfer(s) of the Personal Data[[2]](#footnote-2), or

## the data Processing principles set forth in Annex A.

## Data importer to indicate which option it selects:

## the UK GDPR and DPA 2018, or

1. the data processing principles set forth in Annex A.

Initials of data importer:

1. It will not disclose or transfer the Personal Data to a third party data Controller located outside the UK unless it notifies the Data Exporter about the transfer and

## the third party data Controller Processes the Personal Data in accordance with UK adequacy regulations finding that a third country provides adequate protection, or

## the third-party data Controller becomes a signatory to these clauses, or another data transfer agreement approved by the Commissioner, or

## Data Subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

## with regard to onward transfers of sensitive data, Data Subjects have given their unambiguous consent to the onward transfer.

1. **Liability and third party rights**
2. Each Party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a Party for its outrageous conduct) are specifically excluded. Each Party shall be liable to Data Subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under the UK GDPR or the DPA 2018..
3. The Parties agree that a Data Subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his Personal Data, and accept jurisdiction for this purpose in the Data Exporter’s country of establishment. In cases involving allegations of breach by the Data Importer, the data subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).
4. **Law applicable to the clauses**

These clauses shall be governed by the law of the country in which the Data Exporter is established, with the exception of the laws and regulations relating to Processing of the Personal Data by the Data Importer under clause II(h), which shall apply only if so selected by the Data Importer under that clause.

1. **Resolution of disputes with Data Subjects or the the Commissioner**
2. In the event of a dispute or claim brought by a data subject or the UKEF concerning the Processing of the Personal Data against either or both of the parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
3. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Commissioner. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
4. Each Party shall abide by a decision of a competent court of the Data Exporter’s country of establishment or of the Commissioner which is final and against which no further appeal is possible.
5. **Termination**
6. In the event that the Data Importer is in breach of its obligations under these clauses, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the Contract is terminated.
7. In the event that:
8. the transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to paragraph (a);
9. compliance by the Data Importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
10. the Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
11. a final decision against which no further appeal is possible of a competent court of the Data Exporter’s country of establishment or of the United Kingdom’s rules that there has been a breach of the clauses by the Data Importer or the Data Exporter; or
12. a petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these clauses, in which case the Commissioner shall be informed where required. In cases covered by (i), (ii), or (iv) above the Data Importer may also terminate these clauses.

1. Either Party may terminate these clauses if new UK adequacy regulations under Section 17A Data Protection Act 2018 are issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the Data Importer.
2. The Parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the Processing of the Personal Data transferred.
3. **Variation of these clauses**

The Parties may not modify these clauses except to update any information in Annex B, in which case they will inform the Commissioner where required. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding additional commercial clauses where required.

1. **Description of the Transfer**

The details of the transfer and of the Personal Data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The Parties may execute additional annexes to cover additional transfers, which will be submitted to the Commissioner where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FOR DATA IMPORTER FOR DATA EXPORTER ............................................................ …………………………………………

............................................................ …………………………………………

............................................................ …………………………………………

*Annex A*

**DATA PROCESSING PRINCIPLES**

1. Purpose limitation: Personal Data may be Processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the Data Subject.
2. Data quality and proportionality: Personal Data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further Processed.
3. Transparency: Data Subjects must be provided with information necessary to ensure fair Processing (such as information about the purposes of Processing and about the transfer), unless such information has already been given by the Data Exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data Controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the Processing. Any person acting under the authority of the data Controller, including a Processor, must not Process the data except on instructions from the data Controller.
5. Rights of access, rectification, deletion and objection: Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter.

Provided that the Commissioner has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organisations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the Personal Data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated.

Data Subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or Processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the Processing of the Personal Data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the Data Subject may always challenge a refusal before the Commissioner.

1. Sensitive Data: The Data Importer shall take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under clause II.
2. Data used for marketing purposes: Where data are Processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to “opt-out” from having his data used for such purposes.
3. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated Processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning Data Subjects, except when:
   1. (i) such decisions are made by the Data Importer in entering into or performing a contract with the Data Subject, and

(ii) (the Data Subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

Or

* 1. where otherwise provided by the law of the Data Exporter.

*ANNEX B*

**DESCRIPTION OF THE TRANSFER**

*(To be completed by the parties)*

**Data Subjects**

The Personal Data transferred concern the following categories of Data Subjects:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Purposes of the transfer(s)**

The transfer is made for the following purposes:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Categories of data**

The Personal Data transferred concern the following categories of data:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Recipients**

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Sensitive Data** (if appropriate)

The Personal Data transferred concern the following Categories of Sensitive Data:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Data protection registration information of Data Exporter** (where applicable)

……………………………………………………………………………………………………………………………………………………………………………………………………

**Additional useful information** (storage limits and other relevant information)

……………………………………………………………………………………………………………………………………………………………………………………………………

**Contact points for data protection enquiries**

**Data importer Data Exporter**

............................................................... ……..……………………………………

............................................................... ……..……………………………………

............................................................... ……..……………………………………

**Annex 4 - Transfer of personal data from the UK to processors established in third countries (controller-to-processor transfers).**

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the Personal Data specified in Annex A to this Annex 4.

1. **Definitions**

For the purposes of the Clauses:

**(a)** **personal data**, **special categories of data**, **process/processing**, **controller**, **processor**, **data subject** and **Commissioner**  shall have the same meaning as in the UK GDPR;

**(b)** **the data exporter** means the controller who transfers the personal data;

**(c)** **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

**(d)** **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

**(e)** **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

**(f)** **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

1. **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in ANNEX A1 which forms an integral part of the Clauses.

1. **Third-party beneficiary clause**
2. The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.
3. The data subject can enforce against the data importer this clause 3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
4. The data subject can enforce against the sub-processor this clause3(c), clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
5. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.
6. **Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in ANNEX B to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of ANNEX B and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with clause 4(a) to clause 4(i).

1. **Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in ANNEX B before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner ;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of ANNEX B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

1. **Liability**
   1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
   2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

1. **Mediation and jurisdiction** 
   1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner ;

(b) to refer the dispute to the UK courts.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

1. **Cooperation with supervisory authorities**
   1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
   2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
   3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).
2. **Governing Law**

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established.

1. **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clauses.

1. **Sub-processing**
   1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
   2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
   3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the data exporter is established.
   4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner .
2. **Obligation after the termination of personal data processing services**
   1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
   2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

**ANNEX A**

The Parties may complete or specify, according to their national procedures, any additional necessary information to be contained in this ANNEX A.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Controller** | |  | | |
| The data controller is | |  | | |
| **Data exporter** | |  | | |
| The data exporter is (please specify briefly your activities relevant to the transfer): | |  | | |
| **Data importer** | |  | | |
| The data importer is (please specify briefly your activities relevant to the transfer): | | *Insert* | | |
| **Sub-processor** | |  | | |
| The sub-processor is | |  | | |
| **Data subjects** | |  | | |
| The personal data transferred concern the following categories of data subjects (please specify) | |  | | |
| **Categories of data** | |  | | |
| The personal data transferred concern the following categories of data (please specify) | | • Names  • Company address  • Personal email (business)  • Telephone (business)  • Mobile (business)  and all other Personal Data (as defined in the UK GDPR) | | |
| **Special categories of data (if appropriate)**  The personal data transferred concern the following special categories of data (please specify)  **[Guidance: for the purposes of the SCC special categories includes:**  racial or ethnic origin political opinions religious or philosophical beliefs trade union membership genetic data biometric data (if used to identify a natural person) health sex life or sexual orientation criminal convictions and offencesIf this doesn’t apply please delete the special categories]. | | | |  |
|  |
| **Processing operations** The personal data transferred will be subject to the following basic processing activities (please specify):[Guidance: this section requires the buyer to list the processing activities which may be carried out. Below are some examples from the ICO. The buyer will need to think about how the data importer will be using and handling the set of personal data transferred to it. If this is unlikely to apply this can be deleted.☐ Receiving data, including collection, accessing, retrieval, recording, and data entry☐ Holding data, including storage, organisation and structuring☐ Using data, including analysing, consultation, testing, automated decision making and profiling☐ Updating data, including correcting, adaptation, alteration, alignment and combination☐ Protecting data, including restricting, encrypting, and security testing☐ Sharing data, including disclosure, dissemination, allowing access or otherwise making available☐ Returning data to the data exporter or data subject☐ Erasing data, including destruction and deletion **☐ Other (please provide details of other types of processing).]** [insert] | | |  | |
| DATA EXPORTER | | DATA IMPORTER | | |
| Name:..................................................  Authorised signature:........................... | | Name:..................................................  Authorised signature:........................... | | |

**ANNEX B**

## [Guidance: UKEF will need to complete the checklist, adding in additional details which are relevant. The checklist includes the baseline security measures that any business (small or large) should implement to protect its data/systems.

## It is unlikely to be appropriate if the data importer is providing IT, digital, technology or telecom processor services.

## This checklist for use where the transfer to the data importer and its processing of the personal data does not cause a particularly high risk to the rights of individuals. For example, where the personal data transferred is:

* **not special category data;**
* **not criminal convictions and offences data;**
* **not personal details issued as an identifier by a public authority;**
* **not bank account, credit card or other payment data; and**
* **not a large volume of data.**

## Consider each statement, and the relevant guidance set out below, and click in the box next to those statements which apply.

## Add supplementary notes to provide any further relevant detail of those security measures.]

## This Annex forms part of the Clauses and must be completed and signed by the Parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The following checklist and supplementary details set out the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

**We use firewalls to protect our internet connection** This will be your first line of defence against an intrusion from the internet.

Supplementary details of firewalls used (add any relevant details):

**We choose the most appropriate secure settings for our devices and software** Most hardware and software will need some level of set-up and configuration in order to provide effective protection.

Supplementary details of security settings used (add any relevant details):

**We control who has access to your data and services** Restrict access to your system to users and sources you trust.

Supplementary details of how access to your system is controlled (add any relevant details):

**We protect ourselves from viruses and other malware?** Anti-virus products can regularly scan your network to prevent or detect threats.

Supplementary details of antivirus and malware protection used (add any relevant details):

**We keep our software and devices up-to-date** Hardware and software needs regular updates to fix bugs and security vulnerabilities.

Supplementary details of how software and devices are kept up to date (add any relevant details, including details of the software packages, cloud services and devices you use in processing the personal data transferred, and how you keep those updated):

**We regularly backup our data** Regular backups of your most important data will ensure it can be quickly restored in the event of disaster or ransomware infection.

Supplementary details of how data is backed up (add any relevant details):

|  |  |
| --- | --- |
| DATA EXPORTER | DATA IMPORTER |
| Name:..................................................  Authorised signature:........................... | Name:..................................................  Authorised signature:........................... |

1. “Relevant provisions” means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses). [↑](#footnote-ref-1)
2. However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the adequacy regulations selected. [↑](#footnote-ref-2)