UK GDRP Data Protection Appendix

Jan 2021

This Data Protection Addendum shall form an appendix ("**Appendix**") to any agreement (the "**Principal Agreement**") between Advocates for International Development, a registered charity (No 1118565) and a company limited by guarantee without share capital (No 05907641) in England and Wales, whose registered business address at The Green House, 244-254 Cambridge Heath Road, London, E2 9DA ("**A4ID**") and any third party **(**"**Third Party**"**)** acting on its own behalf and as agent for each Third Party Affiliate.

The terms used in this Appendix shall have the meanings set forth in this Appendix. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties agree that the terms and conditions set out below shall be added as an Appendix to the Principal Agreement. Except where the context requires otherwise, references in this Appendix to the Principal Agreement are to the Principal Agreement as amended by, and including, this Appendix.

1. **Definitions**
   1. In this Appendix, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:
      1. "**Applicable Laws**" means (a) UK laws on A4ID Personal Data in respect of which A4ID is subject to UK Data Protection Laws; and (b) any other applicable law with respect to any A4ID Personal Data to which A4ID is subject to any other Data Protection Laws;
      2. "**A4ID Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of A4ID pursuant to or in connection with the Principal Agreement;
      3. "**Contracted Processor**" means Third Party or a Subprocessor;
      4. "**Data Protection Laws**" means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
      5. "**UK Data Protection Laws**" means UK GDPR;
      6. "**GDPR**" means UK General Data Protection Regulations;
      7. "**Restricted Transfer**"means:
         1. a transfer of A4ID Personal Data from A4ID to a Contracted Processor; or
         2. an onward transfer of A4ID Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section [[6.4.3](#_Ref483163781) or] [12](#_Ref475892068) below;

* + 1. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Third Party for A4ID pursuant to the Principal Agreement;
    2. "**Standard** **Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section [13.4](#_Ref483203635);
    3. "**Subprocessor**" means any person (including any third party and any Third Party Affiliate, but excluding an employee of Third Party or any of its sub-contractors) appointed by or on behalf of Third Party or any Third Party Affiliate to Process Personal Data on behalf of A4ID in connection with the Principal Agreement; and
    4. "**Third Party Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Third Party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
  1. The terms, "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**","**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
  2. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

1. **Authority**
   1. Third Party warrants and represents that, before any Third Party Affiliate Processes any A4ID Personal Data on behalf of A4ID, Third Party's entry into this Appendix as agent for and on behalf of that Third Party Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Third Party Affiliate.
2. **Processing of A4ID Personal Data**
   1. Third Party and each Third Party Affiliate shall:
      1. comply with all applicable Data Protection Laws in the Processing of A4ID Personal Data; and
      2. not Process A4ID Personal Data other than on A4ID’s documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Third Party or the relevant Third Party Affiliate shall to the extent permitted by Applicable Laws inform the relevant A4ID Group Member of that legal requirement before the relevant Processing of that Personal Data.
   2. A4ID:
      1. instructs Third Party and each Third Party Affiliate (and authorises Third Party and each Third Party Affiliate to instruct each Subprocessor) to:
         1. Process A4ID Personal Data; and
         2. in particular, transfer A4ID Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

* + 1. warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section [3.2.1](#_Ref482951323) on behalf of each relevant A4ID Affiliate.
  1. Annex 1 to this Appendix sets out certain information regarding the Contracted Processors' Processing of the A4ID Personal Data as required the UK GDPR, or equivalent requirements of other Data Protection Laws. A4ID may make reasonable amendments to Annex 1 by written notice to Third Party from time to time as A4ID reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section [3.3](#_Ref482964294)) confers any right or imposes any obligation on any party to this Appendix.

1. **Third Party and Third Party Affiliate Personnel**
   1. Third Party and each Third Party Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the A4ID Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant A4ID Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.
2. **Security**
   1. 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, Third Party and each Third Party Affiliate shall in relation to the A4ID Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the GDPR.
   2. In assessing the appropriate level of security, Third Party and each Third Party Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
3. **Subprocessing**
   1. A4ID authorises Third Party and each Third Party Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section [6](#_Ref472956474) to appoint) Subprocessors in accordance with this section [6](#_Ref472956474) and any restrictions in the Principal Agreement.
   2. Third Party and each Third Party Affiliate may continue to use those Subprocessors already engaged by Third Party or any Third Party Affiliate as at the date of this Appendix, subject to Third Party and each Third Party Affiliate in each case as soon as practicable meeting the obligations set out in section [6.4](#_Ref478107174).
   3. Third Party shall give A4ID prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 4 weeks of receipt of that notice, A4ID notifies Third Party in writing of any objections (on reasonable grounds) to the proposed appointment: neither Third Party nor any Third Party Affiliate shall appoint (nor disclose any A4ID Personal Data to) the proposed Subprocessor except with the prior written consent of A4ID.
   4. With respect to each Subprocessor, Third Party or the relevant Third Party Affiliate shall:
      1. before the Subprocessor first Processes A4ID Personal Data (or, where relevant, in accordance with section [6.2](#_Ref472933585)), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for A4ID Personal Data required by the Principal Agreement;
      2. ensure that the arrangement between on the one hand (a) Third Party, or (b) the relevant Third Party Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for A4ID Personal Data as those set out in this Appendix and meet the requirements of article 28(3) of the GDPR;
      3. if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Third Party, or (b) the relevant Third Party Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes A4ID Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant A4ID Group Member(s) (and A4ID shall procure that each A4ID Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and
      4. provide to A4ID for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Appendix) as A4ID may request from time to time.
   5. Third Party and each Third Party Affiliate shall ensure that each Subprocessor performs the obligations under sections [3.1](#_Ref471379220), [4](#_Ref482964795), [5](#_Ref482964888), [7.1](#_Ref479246263), [8.2](#_Ref482964994), [9](#_Ref464575757) and [11.1](#_Ref482970378), as they apply to Processing of A4ID Personal Data carried out by that Subprocessor, as if it were party to this Appendix in place of Third Party.
4. **Data Subject Rights**
   1. Taking into account the nature of the Processing, Third Party and each Third Party Affiliate shall assist A4ID by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of A4ID's obligations, as reasonably understood by A4ID, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
   2. Third Party shall:
      1. promptly notify A4ID if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of A4ID Personal Data; and
      2. ensure that the Contracted Processor does not respond to that request except on the documented instructions of A4ID or as required by Applicable Laws to which the Contracted Processor is subject, in which case Third Party shall to the extent permitted by Applicable Laws inform A4ID of that legal requirement before the Contracted Processor responds to the request.
5. **Personal Data Breach**
   1. Third Party shall notify A4ID without undue delay upon Third Party or any Subprocessor becoming aware of a Personal Data Breach affecting A4ID Personal Data, providing A4ID with sufficient information to allow A4ID to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
   2. Third Party shall co-operate with A4ID and take such reasonable commercial steps as are directed by A4ID to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
6. **Data Protection Impact Assessment and Prior Consultation**
   1. Third Party and each Third Party Affiliate shall provide reasonable assistance to each A4ID Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which A4ID reasonably considers to be required of any A4ID Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of A4ID Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.
7. **Deletion or return of A4ID Personal Data**
   1. Subject to sections [10.2](#_Ref479850356) and [10.3](#_Ref475523583) Third Party and each Third Party Affiliate shall promptly and in any event within one month of the date of cessation of any Services involving the Processing of A4ID Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those A4ID Personal Data.
   2. Subject to section [10.3](#_Ref475523583), A4ID may in its absolute discretion by written notice to Third Party within one month of the Cessation Date require Third Party and each Third Party Affiliate to (a) return a complete copy of all A4ID Personal Data to A4ID by secure file transfer in such format as is reasonably notified by A4ID to Third Party; and (b) delete and procure the deletion of all other copies of A4ID Personal Data Processed by any Contracted Processor. Third Party and each Third Party Affiliate shall comply with any such written request within one month of the Cessation Date.
   3. Each Contracted Processor may retain A4ID Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Third Party and each Third Party Affiliate shall ensure the confidentiality of all such A4ID Personal Data and shall ensure that such A4ID Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.
   4. Third Party shall provide written certification to A4ID that it and each Third Party Affiliate has fully complied with this section [10](#_Ref472960661) within one month of the Cessation Date.
8. **Audit rights**
   1. Subject to sections [[11.2](#_Ref483162686) to [11.4](#_Ref483162694)], Third Party and each Third Party Affiliate shall make available to A4ID on request all information necessary to demonstrate compliance with this Appendix, and shall allow for and contribute to audits, including inspections, by A4ID or an auditor mandated by A4ID in relation to the Processing of the A4ID Personal Data by the Contracted Processors.
   2. Information and audit rights of A4ID only arise under section [11.1](#_Ref482970378) to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

1. **Restricted Transfers**
   1. Subject to section [12.3](#_Ref483204307), A4ID (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from A4ID to that Contracted Processor.
   2. The Standard Contractual Clauses shall come into effect under section [12.1](#_Ref476316761) on the later of:
   3. the data exporter becoming a party to them;
   4. the data importer becoming a party to them; and
   5. commencement of the relevant Restricted Transfer.
   6. Section [12.1](#_Ref476316761) shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.
2. **General Terms**

*Governing law and jurisdiction*

* 1. Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:
     1. the parties to this Appendix hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Appendix, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
     2. this Appendix and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

*Order of precedence*

* 1. Nothing in this Appendix reduces Third Party's or any Third Party Affiliate’s obligations under the Principal Agreement in relation to the protection of Personal Data or permits Third Party or any Third Party Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Appendix and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
  2. Subject to section [13.2](#_Ref483165090), with regard to the subject matter of this Appendix, in the event of inconsistencies between the provisions of this Appendix and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Appendix, the provisions of this Appendix shall prevail.

*Changes in Data Protection Laws, etc.*

* 1. A4ID may:
     1. by at least thirty calendar days' written notice to Third Party from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section [12.1](#_Ref476316761)), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and
     2. propose any other variations to this Appendix which A4ID reasonably considers to be necessary to address the requirements of any Data Protection Law.
  2. If A4ID gives notice under section [13.4.1](#_Ref483203166):
     1. Third Party and each Third Party Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section [6.4.3](#_Ref483163781); and
     2. A4ID shall not unreasonably withhold or delay agreement to any consequential variations to this Appendix proposed by Third Party to protect the Contracted Processors against additional risks associated with the variations made under section [13.4.1](#_Ref483203166).
  3. If A4ID gives notice under section [13.4](#_Ref483203394), the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in A4ID's notice as soon as is reasonably practicable.
  4. Neither A4ID nor Third Party shall require the consent or approval of any A4ID Affiliate or Third Party Affiliate to amend this Appendix pursuant to this section 13.5 or otherwise.

*Severance*

* 1. Should any provision of this Appendix be invalid or unenforceable, then the remainder of this Appendix shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

**ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA**

This Annex 1 includes certain details of the Processing of A4ID Personal Data as required by Article 28(3) GDPR.

***Subject matter and duration of the Processing of A4ID Personal Data***

The subject matter and duration of the Processing of the A4ID Personal Data are set out in the Principal Agreement.

***The nature and purpose of the Processing of A4ID Personal Data***

The nature and purpose of the Processing of the A4ID Personal Data are set out in the Principal Agreement.

***The types of A4ID Personal Data to be Processed***

The types of A4ID Personal Data that may be Processed include the personal data of those who work for or with Legal Partners, Development Partners, funders, stakeholders, clients, members and partners of A4ID.

The Personal Data may also include data relating to their engagement with A4ID’s main activities, including, but not limited to, the Pro Bono Brokerage, ROLE UK Programme Coordination Activities, Legal Clinics and Secondments, Legal Health Checks, ROLE UK Programme Partnership support, training on law and development, ROLE UK Programme papers, A4ID case studies, testimonials, evidence collection, thought leadership on SDGs including the Legal Guide to the SDGs, the develop of A4ID international offices, and thought Leadership on business and human rights.

The specific types of data may include first and last name, job title, position, employer, contact information including company, email, phone, physical business address, professional life data, recruitment data, and localisation data.

***The categories of Data Subject to whom the A4ID Personal Data relates***

The subject matter and duration of the Processing of the A4ID Personal Data are set out in the Principal Agreement.

***The obligations and rights of A4ID***

The obligations and rights of A4ID are set out in the Principal Agreement.**ANNEX 2: STANDARD CONTRACTUAL CLAUSES**

*These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the UK ICO in compliance with the UK GDPR and Data Protection Act 2018 or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).*

*Where* *these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".*

**Standard Contractual Clauses (processors)**

Name of the data exporting organisation: the details as referred to in the A4ID Data Protection Appendix and the Principal Agreement. (the data **exporter**)

*and*

The Third Party details as referred to in the Principal Agreement.

(the data **importer**)

each a “party”; together “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 Appendix 1.

***Background***

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/ECand applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

*Clause 1*

***Definitions***

For the purposes of the Clauses:

* 1. *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
  2. '*the data exporter'* means the controller who transfers the personal data;
  3. *'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 his instructions and the terms of the Clauses.
  4. *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 his instructions, the terms of the Clauses and the terms of the written subcontract;
  5. '*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 Member State in which the data exporter is established;
  6. *'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.

*Clause 2*

***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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 subprocessor shall be limited to its own processing operations under the Clauses.
4. 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.

*Clause 4*

***Obligations of the data exporter***

The data exporter agrees and warrants:

* 1. 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 relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
  2. 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;
  3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
  4. 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;
  5. that it will ensure compliance with the security measures;
  6. 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 providing adequate protection within the meaning of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.*]
  7. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
  8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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;
  9. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
  10. that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

***Obligations of the data importer***

The data importer agrees and warrants:

* 1. 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;
  2. 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;
  3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
  4. that it will promptly notify the data exporter about:
     1. 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,
     2. any accidental or unauthorised access, and
     3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
  5. 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 supervisory authority with regard to the processing of the data transferred;
  6. 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 supervisory authority;
  7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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;
  8. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
  9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
  10. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***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 subprocessor 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 his subprocessor 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 of 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 subprocessor of its obligations in order to avoid its own liabilities.

1. 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***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:
   1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   2. to refer the dispute to the courts in the Member State in which the data exporter is established.
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.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Subprocessing***

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing 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 data exporter's data protection supervisory authority.

*Clause 12*

***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 subprocessor 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 subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**Appendix 1 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

**Data exporter**

The data exporter is:

Advocates for International Development, a registered charity (No 1118565) and a company limited by guarantee without share capital (No 05907641) in England and Wales, whose registered business address at The Green House, 244-254 Cambridge Heath Road, London, E2 9DA.

**Data importer**

The data importer is:

Any third party **(**"**Third Party**"**)** acting on its own behalf and as agent for each Third Party Affiliate, as set out further in the Principal Agreement.

**Data subjects**

The personal data transferred concern the following categories of data subjects:

Details as per Annex One of the Appendix

**Categories of data**

The personal data transferred concern the following categories of data:

Details as per Annex One of the Appendix

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data:

Details as per Annex One of the Appendix

**Processing operations**

The personal data transferred will be subject to the following basic processing activities:

Details as per Annex One of the Appendix

**Appendix 2 to the Standard Contractual Clauses**

This Appendix 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 data importer uses firewalls to protect our internet connection, as a first line of defence against an intrusion from the internet.

The data importer chooses the most appropriate secure settings for their devices and software, ensuring that both hardware and software are set-up and configured in order to provide effective protection.

The data importer controls who has access to the data and services, restricting access to the system to users and sources that they trust.

The data importer protects itself from viruses and other malware, using anti-virus products to regularly scan their network to prevent or detect threats.

The data importer keeps their software and devices up-to-date, ensuring that their hardware and software are regular updated to fix any bugs and security vulnerabilities.

The data importer regularly backups their data, to ensure that the most important data can be quickly restored in the event of disaster or ransomware infection.