**Guidance Notes – Delete this text box once you’ve read it**

There are several sections to complete on this document:

* The cover sheet
* The detail of the organisation this DSA is with (Page 2, Point 2)
* The table in Section 7 – the grey text has guidance notes but every DSA must have this overwritten with the information that’s relevant for this contract
* Signatures on P10 – the signatory is whoever signs the contract this DSA relates to (it is not the DPO)
* Schedule B on P12

If you need any help, please feel free to ask the Data Protection Office via [dataprotectionofficer.uk@actionaid.org](mailto:dataprotectionofficer.uk@actionaid.org)

**Data Security Agreement**

**ActionAid**

**and**

*insert name here*

DATED ............/............../…………

**Contract Ref. No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**THIS AGREEMENT** is made the ..............day of ......................................

**BETWEEN:**

(1) ActionAid, registered in England and Wales (charity no. 274467) (company no. 1295174 limited by guarantee) and Scotland (charity no. SC045476), of registered address: 33-39 Bowling Green Lane, London EC1R 0BJ (hereinafter known as the **“Data Controller")** and

1. [Company name and address], (hereinafter known as the “Data processor”)
2. That, as part of its service to the Data Controller, it will/will not process any personal data that is in the possession of the Controller.

**WHEREAS**

A. The Data Processor and the Data Controller have entered into a business relationship that is or may be the subject of a number of other Agreements.

B. This Agreement is supplemental to any other separate agreement entered into between the parties and introduces further contractual provisions to ensure the protection and security of data passed from the Data Controller to the Data Processor for processing.

C. The Data Protection Act 2018 and its successors in law, including, but not limited to, the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679), place certain obligations upon a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the processing of the data carried out on its behalf is secure.

D. This Agreement exists to ensure that there are sufficient security guarantees in place and that the processing complies with obligations equivalent to those of the 7th Data Protection Principle, and Articles 5 & 32, plus Recitals 39 & 83 of the General Data Protection Regulation (GDPR) (Regulations (EU) 2016/679).

**IT IS AGREED as follows:**

1. **Definitions**

In this Agreement the following words and phrases shall have the following meanings unless the context otherwise requires:

|  |  |
| --- | --- |
| **Data** | Any personal data and sensitive personal data as defined in the Data Protection Act 2018 and successor legislation, including, but not limited to, the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679), that is supplied by the Data Controller and the Data Processor. “Data” also incorporates the meaning of “Personal Data” given in the Data Protection Laws. |
| **Project** | the business relationship existing between the Data Processor and the Data Controller that is the subject of other Agreements; |
| **Approved Employees**  **Data Controller**  **Data Breach**  **Data Processor**  **Data Laws**  **GDPR** | those employees of the Data Processor (or subcontractors if permitted in the relevant Agreement) who are involved in the processing of data  has the meaning given to 'Data Controller', or 'Controller' as appropriate, in the Data Protection Laws; Controller’ may be alternately referred to as ‘Charity’;  means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to/inability to access, Personal Data transmitted, stored, or otherwise processed;  has the meaning given to 'Data Processor', or 'Processor' as appropriate, in the Data Protection Laws; ‘Processor/Data Processor’ may be alternately referred to as ‘Supplier’;  means any and all laws, statutes, enactments, orders or regulations or other similar instruments of general application and any other rules, instruments or provisions in force from time to time relating to the processing of personal data and privacy applicable to the performance of this Agreement, including where applicable the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and the GDPR (Regulation (EU) 2016/679), as amended or superseded ;  means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC as updated, superseded or repealed from the time to time. |

2. **Security and confidentiality of the Data**

2.1 The Data Processor agrees that all rights in the Data provided to it by the Data Controller are reserved to the Data Controller, and that the Data shall only be processed, reproduced, used, or passed to any other party in accordance with the specific instructions of the Data Controller.

2.2 The Data Processor will not make any use of the Data or allow any use of the Data except for the purpose of the Project and in particular will not use any of the Data for any other commercial purposes.

2.3 The Data Processor will hold the Data in the strictest confidence and will not disclose or allow the disclosure of any part of the Data, save as permitted in sub-clause 2.4 below to any third party without the Data Controller’s prior written consent which may be withheld or given on such terms and conditions as the Data Controller may consider appropriate.

2.4 The Data Processor will restrict access to the Data to such Approved Employees as strictly need to have access for the purpose of the Project and the Data Processor will impose upon all such persons obligations of confidentiality equivalent to those contained in this Agreement and the Data Processor will be responsible for ensuring that all such persons comply with these obligations.

2.5 The Data Processor shall take reasonable steps to ensure the reliability of all Approved Employees. For the avoidance of doubt, if the Data Processor is permitted to sub-contract any part of the services under a particular Agreement, any such sub-contracting shall not relieve the Data Processor of its obligations to comply fully with this Agreement and it shall remain fully responsible and legally liable for ensuring full compliance with this Agreement in all respects.

2.6 The Data Processor shall safeguard the Data from unauthorised or unlawful processing or accidental loss, destruction or damage.

# 3. **Compliance with Data Protection Laws**

The Data Processor warrants that it has complied, and shall continue to comply, with the requirements of the applicable Data Protection Laws and all other data protection legislation in any jurisdiction relevant to the exercise of its rights or the performance of its obligations under this Agreement.

4. **Grounds for Processing**

* 1. The Data Controller shall, for all categories of personal data (including special categories) processed under this Agreement, either:
     1. obtain the consent of the data subject to the processing; or confirm the legal basis upon which the Personal Data is being processed;
     2. confirm the legal basis upon which the Personal Data is being processed.
  2. The Data Controller shall indemnify the Data Processor against all liabilities, costs, expenses, damages and losses (including reasonable professional costs and expenses) suffered or incurred by the Data Processor as a result of the Data Controller's breach of its obligations pursuant to paragraph 4.1 above.

1. **Data Processing Obligations**
   1. In respect of any Personal Data to be processed by the Data Processor pursuant to this Agreement for which the Charity is the Data Controller, the Data Processor shall:
      1. have in place and at all times maintain appropriate technical and organisational measures in such a manner as is designed to ensure the protection of the rights of the data subject and to ensure a level of security appropriate to the risk;
      2. not engage any sub-processor without the prior specific or general written authorisation of the Controller (and in the case of general written authorisation; the Data Processor shall inform the Charity of any intended changes concerning the addition or replacement of other processors and the Charity shall have the right to object to such changes);
      3. ensure that each of the Data Processor's employees, agents, consultants, subcontractors, and sub-processors are made aware of the Data Processor's obligations under this Schedule and enter into binding obligations with the Data Processor to maintain the levels of security and protection required under this Schedule. The Data Processor shall ensure that the terms of this Schedule are incorporated into each agreement with any sub-processor, subcontractor, agent or consultant to the effect that the sub-processor, subcontractor, agent or consultant shall be obligated to act at all times in accordance with duties and obligations of the Data Processor under this Schedule. The Data Processor shall at all times be and remain liable to the Controller for any failure of any employee, agent, consultant, subcontractor or sub­ processor to act in accordance with the duties and obligations of the Data Processor under this Schedule;
      4. process that Personal Data only on behalf of the Controller in accordance with the Charity’s instructions and to perform its obligations under this Agreement or other documented instructions and for no other purpose save to the limited extent required by law;
      5. Upon the request of the Controller, within 30 days of expiry or termination of this agreement, the Processor shall make available to the Controller for secure download a full and complete file of the Charity’s Data. After the expiry of the 30-day period, the Processor shall, unless required otherwise by law, delete all of the Charity’s Data in its systems or otherwise in its possession or control, according to the schedule outlined in **Schedule B**, *Data Deletion Schedule and Reporting*;
      6. ensure that all persons authorised to access the Personal Data are subject to obligations of confidentiality and receive training to ensure compliance with this Agreement and the Data Protection Laws;
      7. make available to the Controller all information necessary to demonstrate compliance with the obligations laid out in Article 28 of GDPR and this Schedule and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; provided that, in respect of this provision the Data Processor shall immediately inform the Charity if, in its opinion, an instruction infringes Data Protection Laws;
      8. taking into account the nature of the processing, provide assistance to the Charity, within such timescales as the Charity may require from time to time, in connection with the fulfilment of the Controller’s obligation as Data Controller to respond to requests for the exercise of data subjects' rights pursuant to Chapter Ill of the GDPR to the extent applicable;
      9. provide the Charity with assistance in ensuring compliance with articles 32 to 36 (inclusive) of the GDPR (concerning security of processing, data breach notification, communication of a personal data breach to the data subject, data protection impact assessments, and prior consultation with supervisory authorities) to the extent applicable to the Charity, taking into account the nature of the processing and the information available to the Data Processor;
      10. immediately notify the Controller in writing about:
2. any Data Breach or any accidental loss, disclosure or unauthorised access of which the Data Processor becomes aware in respect of Personal Data that it processes on behalf of the Charity;
3. any request for disclosure of the Personal Data by a law enforcement authority (unless otherwise prohibited);
4. any access request or complaint received directly from a data subject (without responding other than to acknowledge receipt).
   * 1. maintain a record of its processing activities in accordance with Article 30 of the GDPR; and
     2. indemnify the Charity against all liabilities, claims, costs, expenses, damages and losses damages and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties, and legal and other professional costs and expenses) suffered or incurred by the Charity or for which it may become liable as a result of or in connection with any failure of the Data Processor, its employees, agents, consultants, subcontractors, or sub-processors to comply with this Schedule.
   1. The Data Processor shall, at the Charity’s expense to be calculated based upon the Data Processor's standard hourly charge out rates:
      1. deal promptly and properly with all enquiries or requests from the Controller relating to the Personal Data and the data processing activities, promptly provide to the Charity in such form as the Charity may request, a copy of any Personal Data requested by the Charity; and
      2. assist the Charity (where requested by the Controller) in connection with any regulatory or law enforcement authority audit, investigation or enforcement action in respect of the Personal Data.

# **International Data Transfers**

* 1. In respect of any Personal Data to be processed by a party acting as Data Processor pursuant to this Agreement for which the other party is Data Controller, the Data Processor shall not transfer the Personal Data outside the EEA or to an international organisation without:
     1. obtaining the advance written permission of the Data Controller;
     2. ensuring appropriate levels of protection, including any appropriate safeguards if required, are in place for the Personal Data in accordance with the Data Protection Laws;
     3. notifying the Data Controller of the protections and appropriate safeguards in paragraph 5.1.2, above; and
     4. documenting and evidencing the protections and appropriate safeguards in paragraph 5.1.2 above and allowing the Data Controller access to any relevant documents and evidence.

# **Details of Processing Activities**

* 1. The following table sets out the details of processing as required by Article 28 off GDPR (the Charity and Supplier to provide all answers in right column):

|  |  |
| --- | --- |
| **Purposes for which the Personal Data shall be processed**   * Please specify the purposes for which the Data Processor intends to process the Personal Data. | *.For example:*   * *Marketing* * *Employee records / Payroll* * *Recruitment* * *Outsourced Fundraising*   *List all that are applicable – you may have one or several.* |
| **Description of the categories of the data subjects**   * Please specify the categories of data subject whose   Personal Data shall be processed under this Agreement. | *For example:*   * *Employees (bear in mind that if the processing is for a new system that will have user log ins, you need to include this)* * *Job Applicants* * *Supporters* * *Campaigners* * *The General Public*   *List all that are applicable – you may have one or several.* |
| **Description of the categories of Personal Data**   * Please specify the categories of Personal Data that shall be processed under this Agreement. | *For example:*   * *Contact Details* * *Financial Information – bank, tax, pension details* * *HR Information – leave, performance, employment history* * *Special Categories of data (race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation) If any of these are relevant, they should each be listed.* * *Lifestyle information*   *List all that are applicable – you may have one or several.* |
| **Description of transfers of Personal Data to a country outside of the EEA**   * Please record transfers of Personal Data outside of the EEA, recording the country and/or international organisation and, where applicable, please document suitable safeguards. | *If data is only going to be used or accessible in the EEA, you can put N/A for this section.*  *The EEA is EU member states, plus Iceland, Norway and Lichtenstein.*  *Safeguards applicable to our business at present are:*   * *The country is one that has been found to be adequate: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.* * *The company is based in or their systems are hosted in Canada.* * *The company is US based or their systems are US Hosted, and they are signed up to US Privacy Shield (they should assert this, and you can double check* [*here*](https://www.privacyshield.gov/list)*)* * *The data subject has given their explicit consent to the transfer.* * *The transfer is part of a contract with an individual.*   *You only need one of these safeguards, but if none are in place the contract is unlikely to be able to proceed. You must contact the DPO to discuss this further.* |
| **The envisaged time limits for erasure of the different categories of Personal Data**   * Please specify how long you think the Personal Data will be retained for, where possible. | *Either a time limit or the method for determining the time limit must be stated here. For example “For the duration of the contract, with Personal Data deleted 3 months after the end of the contract.”*  *This time limit should be as short as is practical, but sometimes . If there’s no need to keep data beyond a contract term then we would expect deletion in 30 days as standard.* |
| **General description of technical and organisational security measures**   * Where possible, please describe the measures put in place under Article 32(1) GDPR. | *The supplier will largely complete this section although we may want to include something on data transfer measures ie use of an SFTP.*  *Examples of what we would expect a supplier to list:*   * *Restricted access to systems with data only available to those who need it* * *IT security measures (ie we have Mimecast as part of our protection)* * *Data Protection Training for staff* |
| **Authorised Sub-Processors**   * List the sub-processors who will process Personal Data. | *This is for the supplier to complete.* |

8. **Termination**

Upon termination of a Project or of this Agreement (as the case may be), the Data Processor shall promptly return in a secure fashion to the Data Controller all Data (including copies, and in whatever form it may be) or, on the Data Controller request, shall destroy the Data and certify completion of such destruction in writing.

The undertakings contained in this Agreement shall continue in force and effect and shall ensure for the benefit of the Data Controller notwithstanding the completion of the Project (whether in whole or in part) or until all Data has been returned to the Data Controller (or destroyed upon instruction as noted above).

9. **Warranty**

The Data Controller warrants that it has complied with the provisions of the Data Protection Act 2018 and its successor legislation, including, but not limited to, the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679), in relation to the Data and that all instructions given by the Data Controller to the Data processor will be in compliance with these Acts.

The Data Processor warrants to the Data Controller that:

a) They have appropriate technical and organisational measures in place to protect against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This will include, though need not be limited to, those measures listed in Schedule A of this agreement

b) They will not process personal data that is controlled by the data controller otherwise than on, and in accordance with, the express written instructions of the data controller. All processing carried out by the data processor shall be done in accordance with all provisions of the Data Protection Act 2018 and its successor legislation, including, but not limited to, the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679).

c) The Data Processor undertakes that they will allow the Data Controller, during normal hours and on reasonable notice, to enter their premises for the purpose of verifying the Data Processor’s compliance with the warranties in paragraph a and b above. The Data Processor shall offer the Data Controller all assistance that the data controller may reasonably request for any such visit.

10. **Payment Card Industry Data Security Standard (PCI)**

This clause shall apply only if the Data Processor processes cardholder account and transaction data as part of the Project or service it provides to the Data Controller. The Data Processor:

1. warrants that it is and will remain compliant with PCI security standards; and
2. undertakes to notify the Data Controller forthwith if it loses its PCI accreditation.

11. **Indemnity**

The Data Processor shall be liable for and shall fully indemnify the Data Controller against all claims, demands, actions, costs, proceedings and liabilities of any sort that the Data Controller incurs due to the Data Processor’s (or any sub-contractor’s) breach of this Agreement (including, where applicable, breach of or non-compliance with PCI standards) and the Data Processor shall ensure that it has in place adequate insurance to cover any potential liability under this clause satisfactory evidence of which must be provided to the Data Controller upon request.

12. **Variation and Waiver**

No purported variation of this Agreement shall be effective unless it is in writing and signed by or on behalf of each of the parties. The failure of either party to enforce or to exercise, at any time or for any period of time, any term or any right arising pursuant to this Agreement does not constitute, and shall not be construed as, a waiver of such term or right and shall in no way affect a party’s right to enforce and exercise it.

13. **Governing Law and Jurisdiction**

This Agreement shall be governed by and construed in accordance with English law and the parties shall submit to the exclusive jurisdiction of the English Courts.

**IN WITNESS** whereof the parties have executed this Agreement the day and year first above written.

|  |  |  |  |
| --- | --- | --- | --- |
| **SIGNED** by ……………………………………………….  for and on behalf of the Charity, Action Aid, Data Controller | | )  ) | |
|  | |  | |
|  | |  | |
| **SIGNED** by …………………………………………..……  for and on behalf of **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,**  the Data Processor | )  ) | |

**SCHEDULE A**

**Technical and Organisational Measures**

The Data Processor warrants that:

* 1. Approved SO27001-certified Employees involved in processing Data receive appropriate data protection training and understand their responsibilities under the Act in respect of Data supplied by and/or processed on behalf of the Data Controller.
  2. There is password-controlled access to systems.
  3. There is controlled access to buildings and rooms.
  4. There are adequate precautions against burglary, fire, or natural disaster.
  5. It provides secure destruction of documents containing personal data.
  6. It will back up copies of the data stored securely and separately from the live files.
  7. It has procedures for full deletion before re-use of magnetic media (to prevent possible recovery by an unauthorised party).
  8. Responsibility for the Data Processor’s security policy is clearly placed on a particular person or department.

**SCHEDULE B**

**Data Deletion Schedule and Reporting**