# Data Processing Agreement

Insofar as the Critical Research Corporation ("**Data Processor**") will be processing personal data on behalf of a data controller ("**Data Controller**") in the course of performing CRC Services, the terms of this Data Processing Agreement ("**DPA**") shall apply. Any capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Agreement. In the event of a conflict between any provisions of the Agreement for CRC Services (the "**Agreement**") and this DPA, the provisions of this DPA shall govern and control with regard to the processing of personal data. References to "**Data Protection Laws**" shall mean any law applicable to Data Processor's processing or use of personal data, including (to the extent applicable), 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 ("**GDPR**"), and The California Consumer Privacy Act of 2018, AB375, Title 1.81.5, including any implementing law, as amended ("**CCPA**").

1. **Processing**.
   a) Data Processor will only process, store, and use the personal data it receives from the Data Controller as necessary to provide the Data Processor's services to the Data Controller, the business purposes as set forth in the Agreement, or Data Controller's prior written instructions. The Data Processor shall never retain, use, disclose, sell, or process the personal data other than as specified in the Data Controller's documented instructions or as otherwise permitted by law.

   b) The Data Controller has all necessary rights to provide the personal data to the Data Processor for the processing to be performed in connection with the CRC Services. To the extent required by Data Protection Laws, the Data Controller is responsible for providing all necessary privacy notices to data subjects, and unless another legal basis set forth in the Data Protection Laws supports the lawfulness of the processing, and for obtaining any necessary consents from data subject to the processing required under the Agreement. Should such a consent be revoked by a data subject, the Data Controller will inform the Data Processor of such revocation, and the Data Processor is responsible for implementing Data Controller's instruction with respect to the processing of such personal data.

2. **Confidentiality**.
   The Data Processor shall treat all personal data as Confidential Information under the Agreement, and it shall inform all its employees, agents and approved sub-processors engaged in processing the personal data of the confidential nature of the personal data. The Data Processor shall ensure that all such persons or parties have signed confidentiality agreements with obligations no less restrictive in the use and protection of Confidential Information than those in the Agreement.

3. **Security Measures**.
   a) Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of personal data appropriate to the risk. The Data Processor shall maintain and follow written security policies that are fully implemented and applicable to the processing of personal data. At a minimum, such policies will include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the personal data, conducting appropriate background checks, requiring employees, vendors and others with access to personal data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the personal data aware of information security risks presented by the processing.

   b) At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Article 3 and shall allow the Data Controller to audit and test such measures, to the extent it does not require providing access to other customers' data. Subject to such restriction, the Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller, shall grant the Data Controller´s auditors

reasonable access to any premises and devices involved with the processing of the personal data, and shall provide the Data Controller´s auditors with access to any information relating to the processing of the personal data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this DPA.

4. **Data Transfers**.

Data Processor may transfer personal data across the border to a country outside of the United States, as necessary to provide the Services. Upon request by the Data Controller, Data Processor will provide details of its transfers of EEA personal data outside of the United States.

Solely to the extent Data Controller transfers any personal data from (a) the European Economic Area, or (b) a jurisdiction where a European Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC is in force and covers such transfer, then the parties agree that such personal data is subject to the model contractual clauses attached hereto as Appendix 1 and annexed to Commission Decision 2004/915/EC (the "**Clauses**"), which are hereby incorporated into the Agreement. In such cases, Data Controller is the 'data exporter' and Data Processor is the 'data importer' as defined in the Clauses.

5. **Security Breach**.
The Data Processor will notify the Data Controller without undue delay upon discovery of any suspected or actual security or confidentiality breach or other compromise of personal data, describing the breach in reasonable detail, the status of any investigation or mitigation taken by the Data Processor, and if applicable, the potential number of data subjects affected. Data Processor will not communicate with any third party regarding any security breach except as specified by other party or by applicable law.

6. **Subprocessors**.
The Data Processor may subcontract any of its CRC Services-related activities or allow any personal data to be processed by a third party, provided that such subprocessors are bound by data protection obligations compatible with those of the Data Processor under this DPA.

7. **Data Subject Rights**.
The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Laws.

| **CRITICAL RESEARCH CORPORATION** | **CUSTOMER: [Full legal name]** |
|---|---|
| By: HD Moore | By: _____ |
| Name: HD Moore | Name: _____ |
| Title: CEO | Title: _____ |

## Appendix 1 – Model Clauses

Data Controller and Data Processor 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/A.

### *Clause 1*

### Definitions

'the data exporter' means the controller who transfers the personal data;

'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 and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'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 his instructions, the terms of the Clauses and the terms of the written subcontract;

'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;

'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the trans-mission 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/A 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 sub-processor 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 sub- processor 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:

(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 relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(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 organizational security measures specified in Appendix 1/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 un-lawful destruction or accidental loss, alteration, unauthorized 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 providing adequate protection within the meaning of Directive 95/46/EC;

(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 data protection supervisory authority 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 Appendix 1/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 subject as the data importer under the Clauses; and

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

### *Clause 5*

**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 con-tract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 1/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 unauthorized access; and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 supervisory authority 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, select-ed by the data exporter, where applicable, in agreement with the supervisory authority;

(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 Appendix 1/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;

(j) to send promptly a copy of any sub-processor 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 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 his 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 in-solvent, 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 sub-processor of its obligations in order to avoid its own liabilities.

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.

***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;

   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b. 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 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).

*Clause 9*

**Governing law**

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

*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*

**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 re-main 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 law of the Member State in which the data exporter is established, namely .....

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 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 ser-vices, 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 supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

## Appendix 1/A

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: the non- Critical Research Corporation entity that is a party to the Clauses.

**Data importer**

The data importer is: Critical Research Corporation 1512 Bluebonnet Ln, Austin, TX 78704.

**Data subjects**

The personal data transferred concern the following categories of data subjects: data subjects include individuals about whom data that originated in the EEA is provided to Critical Research Corporation ("**CRC**") via its services by (or at the direction of) the data exporter.

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

- Postal addresses
- Email addresses
- IP addresses
- DNS names
- MAC addresses

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

The personal data transferred concern the following special categories of data (please specify): None

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify): Critical Research Corporation will process the personal data for the purposes of providing its services to the data exporter in accordance with and as described in the Agreement, the DPA, and these Clauses.

## Appendix 1/B

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

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

CRC is committed to implementing appropriate technical and organizational security measures to meet its obligations to the data exporter. CRC has internally documented policies and controls.

These policies refer to all data collected from employees, candidates, users, customers, vendors, or other parties that provide information to CRC.

CRC employees must follow these policies. Contractors, consultants, partners and any other external entities are also covered. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to CRC data.

To help comply with these policies and controls, CRC will:

- Classify all data and apply appropriate controls for each level
- Employ encryption of all customer data in transit and at rest to minimum industry standards
- Perform periodic reviews of all our security policies and controls
- Schedule annual penetration tests of the CRC application and remediate appropriately
- Perform annualized security training for all CRC employees
- Utilize centralized monitoring and logging of all CRC production systems