

Exhibit \_\_\_\_\_

**Data Processing Agreement**

(for use with Controller-Processor Standard Contractual Clauses)

**RECITALS**

This Data Processing Agreement (the “**Data Processing Agreement**”), dated as of [ 1/3/2025 ] (the “**Effective Date**”) by and between [ Minooka CCSD 201 ], a [ school district ] [ Illinois school district, USA ], having its principal place of business at [ 305 W. Church St. Minooka, IL 60447 ] (“**Customer**”), and Baydin Inc, a Delaware Company, having its principal place of business at 147 Castro St, Suite 3, Mountain View CA USA (“**Service Provider**”). This Data Processing Agreement refers to Customer and Service Provider individually as a “**Party**” and collectively as the “**Parties**”.

**WHEREAS**, Customer has subscribed to Service Provider’s Services and has agreed to Service Provider’s online terms of service for such Services (as defined below) (as may have been amended, amended and restated, supplemented, or otherwise modified from time to time in accordance with its provisions) (the “**Terms of Service**”), which defines Service Provider’s obligations with respect to the provision of Services to Customer;

**WHEREAS**, the Service Provider will be processing personal data as part of delivering the Services;

**WHEREAS**, it is therefore necessary for the Parties to enter into an appropriate data processing agreement which reflects the roles of the Parties and their obligations under applicable Data Protection Laws and the Parties wish to enter into such an agreement.

**AGREEMENT**

**NOW, THEREFORE**, in consideration of the premises set out above and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows.

1. **DEFINITIONS.** Capitalized terms used and not defined in this Data Processing Agreement have the respective meanings assigned to them in the Terms of Service.

“**Affiliate**” shall mean any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the Party. For purposes of this definition, the term “control” means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

“**Applicable Law**” shall mean all regional, national, and international laws, rules, regulations, and standards including those imposed by any governmental or regulatory authority which apply from time to time to the person or activity in the circumstances in question.

“**Auditor**” has the meaning set forth in Section 14.2.

“**Controller**” has the meaning set forth in the applicable Data Privacy Law.

“**Customer**” has the meaning set forth in the Preamble.

“**Customer Data**” shall mean any Personal Data that Service Provider processes as a Processor in providing the Services to a Customer pursuant to the Terms of Service.

“**Data Privacy Law**” means, as the case may be, the EU Data Protection Directive 95/46/EC (the “**Directive**”) or, when applicable, EU General Data Protection Regulation 2016/679 (“**GDPR**”), the implementing acts of the foregoing by the Member States of the European Union and/or any other applicable law or regulation relating to the protection of Personal Data, personally identifiable information or protected health information.

“**Data Processing Agreement**” has the meaning set forth in the Preamble.

“**Data Subject**” has the meaning set forth in the applicable Data Privacy Law.

“**Effective Date**” has the meaning set forth in the Preamble.

“**Member State**” means a member state of the European Union and/or the European Economic Area, as may be amended from time to time.

“**Party**” has the meaning set forth in the Preamble.

“**Personal Data**” has the meaning set forth in the applicable Data Privacy Law.

“**Process**” has the meaning set forth in the applicable Data Privacy Law.

“**Processing**” has the correlative meaning to Process as set forth in the applicable Data Privacy Law.

“**Processor**” has the meaning set forth in the applicable Data Privacy Law.

“**Security Incident**” has the meaning set forth in Section 7.1.

“**Service Provider**” has the meaning set forth in the Preamble.

“**Services**” means the provision of services or other work products by the Service Provider as described and set out in the Terms of Service, and such other services as the Parties may agree upon in writing from time to time.

“**Terms of Service**” has the meaning set forth in the Preamble.

“**Standard Contractual Clauses**” has the meaning set forth in Section 11.

“**Subprocessor**” means a third party, other than an Affiliate, engaged by Service Provider to assist with the provision of the Services which involves the processing of Customer Data.

“**Term**” is the term of the Terms of Service.

2. **RELATIONSHIP WITH TERMS OF SERVICE.** Unless there is any conflict or inconsistency between the provisions in the Terms of Service and this Data Processing Agreement (in which case, to the extent this Data Processing Agreement requires additional, more stringent, or more protective obligations, the provisions of this Data Processing Agreement take precedence), all other provisions of the Terms of Service apply. In case of a conflict or inconsistency between the operative provisions in this Data Processing Agreement and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall supersede and take precedence.
3. **STATUS OF PARTIES.** Service Provider is the Processor of Customer Data and Customer is the Controller of Customer Data under this Data Processing Agreement. Service Provider shall not assume any responsibility for determining the purposes for which Customer Data shall be processed.
4. **SCOPE OF DATA PROCESSING.**
  - 4.1. All Parties shall comply with their applicable obligations under Data Privacy Laws.

- 4.2. The subject-matter of the data processing to be carried out by the Service Provider is: the provision of Baydin's Services to Customer and Customer End Users.
- 4.3. The duration of the data processing to be carried out by the Service Provider shall be for the Term stated in the Terms of Service.
- 4.4. The nature and purpose of the data processing is to be carried out by the Service Provider is: services to analyze and improve Customer's and Customer's users' writing style, manage their email, and schedule emails as may be further described in the Terms of Service.
- 4.5. The type of personal data involved in the data processing is: Contact information for Customer, Customer's users, and third party individuals with whom they communicate with; content and metadata for emails, scheduling, and other similar electronic communications between Customer, Customer's users, and third party individuals with whom they communicate with.
- 4.6. The categories of Data Subjects involved in the data processing are: Customer, Customer's users, and third party individuals with whom they communicate with.

## **5. PROCESSOR OBLIGATIONS.**

- 5.1. The Service Provider shall process Customer Data on behalf of Customer exclusively and only in accordance with the documented instructions received from Customer. Customer may provide the Service Provider with general or specific instructions regarding the data processing provided as part of the Services. Instructions shall be issued in writing or via e-mail.
- 5.2. In the event Service Provider is required under any Applicable Law to process Customer Data in excess of Customer's documented instructions, Service Provider shall immediately notify Customer of such a requirement, unless such Applicable Law prohibits such notification on important grounds of public interest, in which case it will notify Customer as soon as the Applicable Law permits it to do so.
- 5.3. Customer shall only provide instructions to Service Provider that comply with Applicable Law and Customer represents and warrants that Service Provider's Processing in accordance with Customer's instructions shall not cause Service Provider to be in breach of any Applicable Laws.
- 5.4. Service Provider shall promptly notify Customer if Service Provider reasonably believes that an instruction issued Customer would violate any Data Protection Laws.
- 5.5. If the Service Provider cannot provide compliance with this Data Processing Agreement for whatever reason, then it shall promptly inform Customer of its inability to comply, in which case the parties shall negotiate in good faith alternative Processing and, if no other alternative processing is commercially reasonable to the Provider, the Provider may immediately suspend any processing and/or terminate, in whole or in part, the Terms of Service and this Data Processing Agreement pursuant to the Terms of Service.
- 5.6. Upon Customer's request, the Service Provider will promptly cooperate with Customer to enable Customer to: (a) comply with all reasonable requests of access, rectification, and/or deletion of Customer Data arising from a Data Subject; (b) enforce rights of Data Subjects under the Data Privacy Law; and/or (c) comply with all requests from a supervisory authority, including but not limited to in the event of an investigation. All costs of such cooperation shall be borne by Customer.

- 5.7. Service Provider shall provide commercially reasonable assistance to Customer where Customer carries out a data privacy impact assessment relating to Customer Data.
- 5.8. The Service Provider shall notify Customer in the event it receives any request, complaint, or communication relating to Customer's obligations under Data Privacy Laws (including from data protection authorities and/or supervisory authorities). To the extent permitted by Applicable Law, Service Provider shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.
- 5.9. Any data collected pursuant to data analytics or monitoring carried out by Service Provider in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data, which Customer hereby authorizes Service Provider to use solely in accordance with carrying out its obligations under the Terms of Service or this Data Processing Agreement.

## **6. SCOPE MODIFICATIONS.**

- 6.1. In the event that changes in Data Privacy Laws require modifications to the Services, the Parties shall use commercially reasonable efforts to comply with such requirements. If such changes in Data Privacy Laws require structural changes to the Services such that the provision of the Services would otherwise be in breach of such Data Privacy Laws unless such changes are performed, the Parties will discuss in good faith Service Provider's ability to comply and will negotiate and revise the Services accordingly. In the event that Service Provider considers in good faith that it is unable to comply with the required changes, Service Provider shall notify without undue delay Customer and Service Provider may terminate the Terms of Service and/or this Data Processing Agreement on no less than thirty (30) days' prior written notice.
- 6.2. In the event that the Service Provider's compliance with Data Privacy Laws requires the imposition of certain additional contractual obligations under this Data Processing Agreement, the Service Provider shall notify the Customer and both Parties shall in good faith seek to amend this Data Processing Agreement in order to address the requirements under Data Privacy Laws. In the event the affected Parties fail to reach agreement on an amendment to this Data Processing Agreement, then Service Provider may, on no less than thirty (30) days' prior written notice, terminate the Terms of Service and this Data Processing Agreement.
- 6.3. Customer shall notify Service Provider of any faults or irregularities in relation to this Data Processing Agreement that it detects in the provision of the Services.

## **7. SECURITY MEASURES.**

- 7.1. The Service Provider shall take and implement appropriate technical and organizational security and confidentiality measures designed to provide a level of security appropriate to the risk to Customer Data against the accidental or the actual or threatened unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Customer Data (a "**Security Incident**").
- 7.2. Such measures implemented in Section 7.1 shall require the Service Provider to have regard to industry standards and costs of implementation as well as taking into account the nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.
- 7.3. Service Provider shall undertake regular reviews of the technical and organizational measures and the data processing operations connected with the Services to ensure

compliance with the Data Processing Agreement and to consider improving the technical and organizational measures such that they meet or exceed the requirements of the Terms of Service.

- 7.4. The Service Provider shall adopt and maintain a comprehensive written information security policy that describes its policies and procedures to comply with this Section 7 and shall provide a summary of such policy to Customer upon request.
- 7.5. The Service Provider shall implement and maintain policies and procedures to detect and respond to Security Incidents.
- 7.6. For the Term of the Terms of Service, the Service Provider will ensure that all persons authorized to process Customer Data only processes Customer Data in accordance with instructions from Customer (unless required to do otherwise under Applicable Law).

8. **CONFIDENTIALITY.** Service Provider represents and warrants that all persons who have access to Customer Data shall maintain its confidentiality as further set forth herein.

9. **SECURITY INCIDENT NOTIFICATION OBLIGATIONS.**

- 9.1. In the event of a Security Incident arising during the performance of the Services by the Service Provider, the Service Provider shall:
  - (a) notify Customer about the Security Incident without undue delay after becoming aware of the Security Incident;
  - (b) as part of the notification under Section 9.1(a), to the extent reasonable available at the time of notice, provide a description of the Security Incident including the nature of the Security Incident, the categories and approximate number of Data Subjects affected, the categories and approximate number of data records affected, the likely consequences of the Security Incident and the risks to affected Data Subjects;
  - (c) promptly update Customer as additional relevant information set forth in 9.1(b) above become available;
  - (d) take all actions as may be required by Data Privacy Laws;
  - (e) maintain records of all information relating to the Security Incident, including the results of its own investigations and authorities' investigations as well as remedial actions taken; and
  - (f) reasonably cooperate with Customer to prevent future Security Incidents.
- 9.2. Service Provider shall make any information referred to under Section 9.1 available to Customer on request. All such information shall be considered the Confidential Information of Service Provider.

10. **SUBPROCESSORS.**

- 10.1. Controller authorizes Service Provider to appoint (and permit each Subprocessor appointed in accordance with this Section 10 to appoint) Subprocessors in accordance with this Section 10 and any restrictions in the Terms of Service.
- 10.2. Notwithstanding anything to the contrary in this Data Processing Agreement or the Terms of Service, Service Provider may continue to use all Subprocessors (including Affiliates)

already engaged by Service Provider as of the Effective Date, subject to Service Provider promptly meeting the obligations set forth in Section 10.4.

- 10.3. Service Provider shall provide reasonable advanced notification to Customer where Service Provider wishes to engage a Subprocessor to process Customer Data and shall provide, upon Customer's request, the identity and location of the Subprocessor and a description of the processing to be subcontracted or outsourced to such Subprocessor. Where Service Provider wishes to appoint a Subprocessor under this Data Processing Agreement, Service Provider will select the Subprocessor with due diligence and will verify prior to engaging the Subprocessor that such Subprocessor is capable of complying with the obligations of the Service Provider towards Customer, to the extent applicable to the services assigned to that Subprocessor. If, within five (5) days of receipt of such notice, Customer notifies Service Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then Service Provider shall not appoint (or disclose any Customer Data to) the proposed Subprocessor until reasonable steps have been taken to address the reasonable objections raised by Customer, and Customer has been provided with a reasonable written explanation of the steps taken.
  - 10.4. The Service Provider shall enter into a contract with each Subprocessor whereby the Service Provider shall require the Subprocessor to comply with obligations no less onerous than the Service Provider's obligations under this Data Processing Agreement. Service Provider shall ensure the subcontracting agreement with such Subprocessor includes appropriate contractual provisions in accordance with Data Privacy Laws.
  - 10.5. Such subcontracting under this Section 10 shall not release the Service Provider from their responsibility for their obligations under the Terms of Service. The Service Provider shall be responsible for the work and activities of all Subprocessors.
11. **INTERNATIONAL DATA TRANSFERS.** Where there are transfers of Personal Data from a Member State to a country that is not a Member State, the Parties agree and acknowledge that each Party is required to implement policies and procedures to ensure that such data transfers comply with Data Privacy Laws. All such transfers shall only be made pursuant to [the European Commission 2010/87/EU of 5 February 2010 (the "**Standard Contractual Clauses**") entered into between the Parties and attached hereto as Attachment 1/the EU – U.S. Privacy Shield and/or Switzerland – U.S. Privacy Shield/Binding Corporate Rules in accordance with Data Privacy Laws].
12. **RETURN AND DESTRUCTION.**
- 12.1. Without prejudice to any obligations under this Section 13, following termination or expiration of the Terms of Service for whatever reason, Service Provider shall cease processing Customer Data and shall require that all Subprocessors cease processing Customer Data.
  - 12.2. Following termination or expiration of the Terms of Service for whatever reason and having received written confirmation from Customer, Service Provider shall destroy all copies of Customer Data, unless and for the duration Service Provider is permitted to retain such Customer Data in accordance with Applicable Laws. Notwithstanding the foregoing, to the extent it is not commercially reasonable for Service Provider to remove Customer Data from archive or other backup media, Service Provider may retain Customer Data on such media in accordance with its backup or other disaster recovery procedures. In the event Service Provider retains Customer Data after the Term, Service Provider shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Customer Data.

12.3. To the extent feasible, Service Provider shall archive documentation that is evidence of proper Customer Data processing beyond termination or expiration of the Terms of Service and continuing for any period of time in which Service Provider retains Customer Data.

**13. AUDITS.**

13.1. Service Provider shall, upon receiving at least thirty (30) days prior written notice from Customer, submit or procure that its Subprocessors submit (as requested), its or their data processing facilities for a reasonable audit of Processing activities carried out under this Data Processing Agreement, where such audit shall be carried out by an independent third-party auditor mutually agreed upon by the Parties and bound by a duty of confidentiality (“**Auditor**”) and, where applicable, approved by the relevant supervisory authority. Any effort as well as internal and external costs of audits requested by Customer pursuant to this Section 14.2 shall be borne by Customer.

13.2. Service Provider shall provide Customer or Auditor with the necessary information and shall keep the necessary records required for an audit of the processing of Customer Data and will, subject to Applicable Law, provide said documents and/or data media to Customer upon written request.

13.3. Service Provider shall provide reasonable support for any and all audits of Customer or Auditor under this Section 14 and shall contribute to the complete and efficient completion of the audit.

**14. TERMINATION.** The rights of termination for cause as set out in the Terms of Service remain unaffected. The termination or expiration of the Terms of Service for any reason shall cause termination of this Data Processing Agreement.

**15. LIABILITY.** The liability of each Party under this Data Processing Agreement shall be subject to the exclusions and limitations of liability set out in the Terms of Service. Any reference to any “limitation of liability” of a party in the Terms of Service shall be interpreted to mean the aggregate liability of a Party and all of its Affiliates under the Terms of Service and this Data Processing Agreement.

**16. MISCELLANEOUS.**

16.1. **Amendment.** This Data Processing Agreement may not be amended or modified except in writing signed by authorized representatives of both Parties.

16.2. **Severability.** If any provision in this Data Processing Agreement is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the Data Processing Agreement and the Terms of Service shall not be affected. The Parties shall promptly and in good faith replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly promptly and in good faith add any necessary appropriate provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this Data Processing Agreement is subject.

16.3. **Governing Law.** Notwithstanding anything to the contrary in the Terms of Service, this Data Processing Agreement shall be governed by and construed in accordance with the national law that applies to the Controller.

- 16.4. **Severability.** If any provision of this Data Processing Agreement is invalid, illegal, or unenforceable by any court or administrative body of competent jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Data Processing Agreement and all such other terms and provisions shall remain in full force and effect. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties shall negotiate in good faith to modify this Data Processing Agreement so as to effect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the Processing contemplated hereby be consummated as originally contemplated to the greatest extent possible.
- 16.5. **Headings.** The headings in this Data Processing Agreement are for reference only and shall not affect the interpretation of this Data Processing Agreement.

[Remainder of page intentionally left blank]



**IN WITNESS WHEREOF**, the Parties have caused their respective duly authorized representatives to execute this Data Processing Agreement, which is effective as of the Effective Date.

Signature: \_\_\_\_\_

Printed Name: Aaron Souza

Title: Director of IT

Date: 01/03/2025

Signature:  \_\_\_\_\_

Printed Name: Alexander Moore

Title: Chief Executive Officer

Date: June 6, 2018

**Attachment 1**

**Commission Decision C(2010)593  
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: ..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

.....  
(the data **exporter**)

And

Name of the data importing organisation: Baydin, Inc.

Address: 147 Castro St, Suite 3, Mountain View, CA, 94041

e-mail: support@baydin.com

Other information needed to identify the organisation:

.....  
(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.

## Clause 1

### **Definitions**

For the purposes of the Clauses:

- (a) *'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;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with 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;
- (d) *'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;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## 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:

- (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 organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) 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;
- (h) 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;

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

#### *Clause 5*

#### ***Obligations of the data importer<sup>1</sup>***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the 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

---

<sup>1</sup> Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

qualifications bound by a duty of confidentiality, selected 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 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;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor 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 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:

- (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 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, 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*

***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<sup>2</sup>. 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, namely .....  
.....  
.....
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.

---

<sup>2</sup> This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.



**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)


**On behalf of the data importer:**

Name (written out in full): Alexander Moore

Position: Chief Executive Officer

Address: 147 Castro St, Suite 3, Mountain View, CA 94041

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

## **APPENDIX 1 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) (or document/legislation attached):**

### Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password and multi-factor/one-time-password secondary security features);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user-master data procedures per data processing environment; and
- Encryption of archived data media.

### Data Access Control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights;
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

### Disclosure Control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

### Entry control

Technical and organizational measures to monitor whether Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Internal Policies and Procedures
- Logging and reporting systems

### Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Redundant storage;
- Remote storage;
- Anti-virus/firewall systems

Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be Processed separately include:

- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes