



## DATA PROCESSING AGREEMENT

*Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU – Standard Contractual Clauses (Processors)*

This Data Processing Agreement (“**DPA**”) forms part of the master agreement between Raygun, Limited (“**Vendor**”) acting on its behalf and as agent of each Vendor Affiliate, and Customer (“**Company**”) acting on its own behalf and as agent for each Company Affiliate (the “**Agreement**”) to reflect the parties’ agreement with regard to the Processing of Personal Data of Customer, in accordance with the requirements of Data Protection Laws.

### APPLICATION OF THIS DPA

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Raygun entity (i.e., either Raygun, Limited or a subsidiary of Raygun, Limited) that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with Raygun or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Raygun entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

### HOW TO EXECUTE THIS DPA:

1. This DPA consists of distinct parts: set of definitions and provisions and this body, the Standard Contractual Clauses, Annex 1 and Appendices 1-2.
2. This DPA has been pre-signed on behalf of Raygun as the data importer.
3. To complete this DPA, Customer must: (a) Complete the information and sign page 9 (b) Annex 1, Standard Contractual Clauses on page 10 (c) Complete the information as a data exporter on Page 17 and sign (d) Complete the information in the signature box and sign on Pages 19-20.
4. Customer must send the completed and signed DPA to Raygun by email at [DPA@raygun.com](mailto:DPA@raygun.com). Upon receipt of the validly-completed DPA by Raygun at this email address, this DPA shall come into effect and legally bind the parties.

### DPA TERMS

#### 1. Definitions

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

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



- 1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:
- 1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;
  - 1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
  - 1.1.3 "**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data;
  - 1.1.4 "**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller, including as applicable, any "service provider" as that term is defined by the CCPA;
  - 1.1.5 "**Personal Data**" means any information relating to an identified or identifiable person where such data is submitted to the Raygun Products as Customer Data;
  - 1.1.6 "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
  - 1.1.7 "**Raygun Products**" means any Software product described in the Agreement;
  - 1.1.8 "**Standard Contractual Clauses**" or "**Clauses**" means the agreement executed by and between Customer and Vendor and attached hereto as Annex 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection;
  - 1.1.9 "**Sub-processor**" means any Data Processor engaged by Vendor and any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Agreement;
  - 1.1.10 "**Contracted Processor**" means Vendor or a Subprocessor;
  - 1.1.11 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
  - 1.1.12 "**EEA**" means the European Economic Area;



- 1.1.13 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
  - 1.1.14 "GDPR" means EU General Data Protection Regulation 2016/679;
  - 1.1.15 "Services" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Agreement;
  - 1.1.16 "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
- 1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## 2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this DPA as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

## 3. Processing of Personal Data

### 3.1 Vendor and each Vendor Affiliate shall:

- 3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
- 3.1.2 Customer's Processing of Personal Data. Customer shall, in its use of Raygun Products, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired such Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.
- 3.1.3 Vendor Processing of Personal Data. Vendor shall only Process Personal Data on behalf of and in accordance with Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs Vendor to Process Personal Data for the purpose of providing the services offered by Vendor, namely diagnosis of software faults and/or analysis and diagnosis of application or infrastructure performance issues.

## 4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those

individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## **5. Security**

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

## **6. Subprocessing**

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this DPA, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

Neither Vendor nor any Vendor Affiliate shall appoint (or disclose any Company Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Company Group Member and Company has been provided with a reasonable written explanation of the steps taken.

6.4 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand, the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR;

- 6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and
- 6.4.4 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Company may request from time to time.
- 6.5 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 9 and 11, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Vendor.
- 7. Data Subject Rights**
- 7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 7.2 Correction, Blocking and Deletion. To the extent Customer, in its use of Raygun Products, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Processing Laws and Regulations, Vendor shall comply with any commercially reasonable request by Customer to facilitate such actions by Customer to the extent Vendor is legally permitted to do so.
- 7.3 Vendor shall:
- 7.3.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
- 7.3.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.
- 8. Data Protection Officer**
- 8.1 Raygun has appointed a Data Protection Officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at [DPA@raygun.com](mailto:DPA@raygun.com).



## 9. Sub-processors

- 9.1.1 Appointment of Sub-processors. Customer acknowledges and agrees that Vendor may engage third-party Sub-processors in connection with the provision of Raygun Products.
- 9.1.2 Liability. Vendor shall be liable for the acts and omissions of its Sub-processors to the same extent Vendor would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

## 10. Personal Data Breach and Notification

- 10.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 10.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## 11. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

## 12. Deletion or return of Company Personal Data

- 12.1 Subject to sections 12.2 and 12.3 Vendor and each Vendor Affiliate shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.
- 12.2 Subject to section 12.3, Company may in its absolute discretion by written notice to Vendor within 30 days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 30 days of the Cessation Date.
- 12.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.



12.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 12 within 30 days of the Cessation Date.

### **13. Audit rights**

13.1 Subject to sections 13.2 to 13.3, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

13.2 Information and audit rights of the Company Group Members only arise under section 13.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

13.3 A Company Group Member may only mandate an auditor for the purposes of section 13.1 if the auditor is identified and agreed with the Vendor at the time of execution of this agreement or agreed in writing in advance of the audit. Vendor shall not unreasonably withhold or delay agreement to the addition of a new auditor.

13.4 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

13.4.1 to any individual unless he or she produces reasonable evidence of identity and authority;

13.4.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

13.4.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

13.4.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this DPA; or

13.4.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

## 14. General Terms

### *Governing law and jurisdiction*

14.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

14.1.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.1.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement; and

14.1.3 unless stated otherwise in the Agreement, the Clauses shall be governed by the law of the Member State in which the data exporter is established.

### *Order of precedence*

14.2 Nothing in this DPA reduces Vendor's or any Vendor Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.3 Subject to section 14.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

### *Changes in Data Protection Laws, etc.*

14.4 Company may:

14.4.1 by at least 30 (thirty) calendar days' give written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

14.4.2 propose any other variations to this DPA which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

14.5 If Company gives notice under section 14.4.1:

14.5.1 Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and





- 14.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 14.4.1 and/or 14.5.1.
- 14.6 If Company gives notice under section 14.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.
- 14.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this DPA pursuant to this section 14.5 or otherwise.

*Severance*

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

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

**[Company]**

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date Signed \_\_\_\_\_

**Raygun Limited**

Signature: 

Name: John-Daniel Trask

Title: CEO / Co-Founder

Date Signed: 4 September 2019



**ANNEX 1: STANDARD CONTRACTUAL CLAUSES**

The Standard Contractual Clauses. The standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and United Kingdom, which have signed Order Forms for the Service. For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed “data exporters.”

**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

Raygun Limited and affiliates:

Address: PO Box 19057, Marion Square, Wellington 6141, New Zealand

Tel.: (206) 508 - 7144; e-mail: [DPA@raygun.com](mailto:DPA@raygun.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.

## Background

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

### *Clause 1*

#### ***Definitions***

For the purposes of the Clauses:

- (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***

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 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.

*Clause 10*

***Variation of the contract***

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

*Clause 11*

***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal



data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

**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.....

**On behalf of the data importer:**

Name: John-Daniel Trask

Position: CEO / Co-Founder

Address: PO Box 19057, Marion Square, Wellington 6141, New Zealand

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

Signature: 



## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### **Data exporter**

The data exporter is:

Data exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) that have purchased or have access to Raygun Products.

### **Data importer**

The data importer is:

The data importer receives data that is sent by the data exporter.

The data importer, Raygun is hosted in the United States, specifically in an Amazon AWS datacenter located in the US-EAST region. AWS has obtained approval from EU data protection authorities, known as the Article 29 Working Party, of the AWS Data Processing Addendum and Model Clauses to enable transfer of data outside Europe, including to the U.S. More information on AWS's privacy can be found at <https://aws.amazon.com/privacy/> and more information on their data privacy, including specific mention of data transfer from the EU can be found here: <https://aws.amazon.com/compliance/data-privacy-faq/>

### **Data subjects**

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

Data exporter may submit Personal Data to the Raygun Products, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- a. Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- b. Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- c. Employees, agents, advisors, independent contractors of data exporter (who are natural persons)
- d. Data exporter's authorized users (individuals authorized by data exporter to use the Raygun Products)

**Categories of data**

The personal data transferred concern the following categories of data:

Data exporter may submit Personal Data to the Raygun Products, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Customer information:

- o User's first and last name
- o User's email address
- o User's IP address

Company information:

- o Business contact information (company, email, phone, physical business address)
- o Personal contact information (email, phone)
- o Title
- o Position
- o Employer
- o Connection data

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

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

Data exporter may submit special categories of data to the Raygun Products, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

**Processing operations**

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

The objective of Processing of Personal Data by data importer is the performance of the Raygun Products pursuant to the Agreement.


**DATA EXPORTER**

Name: .....

Authorised Signature .....

**DATA IMPORTER**

Name: Raygun Limited

Authorised Signature: 

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

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

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Raygun Products. Raygun is and will remain HIPAA compliant.

The list of subprocessors approved by the data importer as of the effective date of the DPA is as set forth below:

Subprocessor	Description of Processing
Amazon Web Services, Inc.	Hosting
Salesforce.com, Inc.	Service Cloud and collaboration tool
Intercom	Support & Maintenance ticketing process
Google (G Suite)	Analytics, email, & document platform
Auto Pilot	Marketing tool
Looker	Business intelligence application software
Slack	Team based instant messaging tool
Xero	Accounting software
Taxify	US state sales tax tool
Zen Desk	Support & maintenance ticketing tool
Stitch	Data management tool
Box.com	File management system
Front	Shared inbox management tool
Productboard	Product management tool
Windcave	Payment gateway platform
Microsoft 365	Microsoft Office software platform

**DATA EXPORTER**

Name: .....

Authorised Signature .....

**DATA IMPORTER**

Name: Raygun Limited

Authorised Signature: 