Schedule 1:

Data Processing Agreement ("DPA")

BACKGROUND:

(A) Customer and Supplier **(Intruder)** are parties to an agreement to which this Data Processing Agreement (the "**DPA**") is incorporated as a schedule (the "**Agreement**"), and under which Agreement Supplier has been engaged by Customer to provide certain services (the "**Services**");

(B) In order to supply all or part of the Services, Supplier will be required to Process certain Personal Data on behalf of Customer;

(C) Accordingly, the parties agree that this DPA sets out the basis on which any Personal Data is Processed in connection with the Agreement;

(D) In the case of any conflict between the terms of the Agreement and this DPA, this DPA will take precedence, and shall supersede any provisions relating to the processing of personal data in the Agreement.

1 DEFINITIONS AND INTERPRETATION

1.1 Unless otherwise defined in this DPA, words and expressions used in this DPA shall have the meanings given in the Agreement. In this DPA the following words should have the following meanings:

"Adequacy Framework"
shall mean any system of certification adopted by the European Commission (or in respect of Personal Data transfers caught by the UK GDPR or the Swiss FADP, the relevant UK and/or Swiss governmental or regulatory body), pursuant to which transfers of Personal Data to participating organisations are considered adequate under Article 45(1) of the GDPR, including the EU-US Data Privacy Framework adopted pursuant to European Commission Implementing Decision of 10 July 2023 (and any equivalent frameworks adopted for the purposes of the UK GDPR and/or the Swiss FADP);

"Customer Personal Data"
shall mean Personal Data:

(a) supplied to Supplier by or on behalf of Customer; and/or

(b) obtained by, or created by, Supplier on behalf of Customer in the course of delivery of Services,

and in each case where such Personal Data is Processed by Supplier for and on behalf of the Customer in the performance of Services (as set out in Schedule 1);

"Data Privacy Laws"
shall mean the following as amended, extended, re-enacted or replaced from time to time:

(a) UK Data Protection Act 2018 and the UK GDPR;

(b) EC Regulation 2016/679 (the "**GDPR**") on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data;

(c) EC Directive 2002/58/EC on Privacy and Electronic Communications;

(d) the Swiss Federal Act on Data Protection 2020 ('**Swiss FADP**");

(e) all local laws or regulations implementing or supplementing the EU legislation mentioned in (b)-(c) above (including the UK Privacy and Electronic Communications Regulations 2003);

(f) all codes of practice and guidance issued by national supervisory authorities, regulators or EU or UK institutions relating to the laws, regulations and EU legislation mentioned in (a)–(e) above;

"EEA"
means the European Economic Area;

"European Law"
means any law in force in the EEA, the United Kingdom, or Switzerland, including the Data Privacy Laws;

"International Transfer Requirements"
means the requirements of Chapter V of the GDPR (Transfers of Personal Data to third countries or international organisations) and/or analogous provisions under Swiss data protection legislation (as applicable);

"Losses"
means losses, damages, liabilities, claims, demands, actions, penalties, fines, awards, costs and expenses (including reasonable legal and other professional expenses);

"Relevant Transfer Mechanism"

shall mean:

(a) in respect of an EU Restricted Transfer (as defined below), the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 ("**EU SCCs**");

(b) in respect of a UK Restricted Transfer (as defined below), the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the ICO under or pursuant to section 119A(1) of the Data Protection Act 2018 (as may be amended by the ICO from time to time pursuant to its terms) ("**UK Addendum**"); or

(c) in respect of a Swiss Restricted Transfer (as defined below), the EU SCCs provided that:

(i) any references in the clauses to the GDPR or EU or Member State Law (or similar) shall refer to the Swiss FADP and/or other relevant Swiss law (as applicable);

(ii) the term 'Member State' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs; and

(iii) the FDPIC is the competent supervisory authority for the purposes of Clause 13 of the EU SCCs ("**Swiss SCCs**");

"Restricted Country"

shall mean:

(a) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission;

(b) where the UK GDPR applies, a country outside the UK which is not subject to an adequacy determination by the UK Government; and

(c) where the Swiss FADP applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the FDPIC.

Such adequacy determinations shall not include adequacy determinations made on the basis of an Adequacy Framework;

"Restricted Transfer"

shall mean a transfer of Personal Data to an entity located in a Restricted Country from an entity whose Processing of such Personal Data is subject to:

(a) the EU GDPR ("**EU Restricted Transfer**");

(b) the UK GDPR ("**UK Restricted Transfer**"); and

(c) the Swiss FADP ("**Swiss Restricted Transfer**"),

but in each case excluding any such transfer made on the basis of an Adequacy Framework;

"UK"

means the United Kingdom; and

"UK GDPR"

has the meaning given to it in the Data Protection Act 2018 (as amended from time to time).

1.2 In this DPA a reference to the GDPR and/or an Article or Chapter of the GDPR shall, where the context so requires and insofar as the Data Privacy Law(s) is that of the UK and/or Switzerland, be construed as a reference to the equivalent Data Privacy Law(s) of the UK and/or Switzerland (as applicable) and/or the corresponding provision of such Data Privacy Law(s).

1.3 Unless the context otherwise requires, a reference to a clause shall be a reference to a clause of this DPA.

1.4 References to "**Processor**", "**Controller**", "**Personal Data**", "**Process**", "**Processing**", "**Personal Data Breach**" "**Data Subject**" or "**Supervisory Authority**" shall have the same meanings as defined in the GDPR.

2 DATA PROTECTION

2.1 Roles of the parties, and processing activities

(a) In relation to all Customer Personal Data, the parties acknowledge and agree that to the extent the Supplier Processes Customer Personal Data on behalf of the Customer in connection with the provision of the Services, the Customer shall be considered a Controller and Supplier shall be considered a Processor.

(b) Each of the parties acknowledges and agrees that the subject-matter and duration of the Processing carried out by the Supplier on behalf of Customer, the nature and purpose of the Processing, the type of Personal

Data and categories of Data Subjects are accurately documented in Schedule 1 to this DPA (which may from time to time be updated by the written agreement of the parties).

(c) If at any time either party considers that the relationship between the parties and/or the scope of Processing carried out by the Supplier no longer corresponds with clause 2.1(a) or (b), that party shall promptly notify the other and the parties shall discuss and agree in good faith such steps that may be required to reflect the true status and/or the scope of Processing undertaken by the Supplier.

2.2 **General obligations of the parties**

Each party shall comply with the obligations imposed on it by applicable Data Privacy Laws with regard to Customer Personal Data Processed by it in connection with Services. Customer acknowledges and agrees that Supplier's compliance with applicable Data Privacy Laws may be dependent on Customer's compliance with applicable Data Privacy Laws and accordingly Supplier will not be liable for failure to comply with applicable Data Privacy Laws where such failure results from a failure of Customer to comply with applicable Data Privacy Laws (including any failure to comply with clause 2.4).

2.3 **Obligations of Supplier**

(a) Supplier shall only Process Customer Personal Data in accordance with the documented instructions of Customer (including those in Schedule 1, as updated), unless required to do so by European Law to which Supplier is subject, in which event Supplier shall inform Customer of such legal requirement unless prohibited from doing so by European Law on important grounds of public interest.

(b) Supplier shall inform Customer if, in Supplier's opinion, an instruction given by Customer to Supplier under clause 2.3(a) infringes the Data Privacy Laws.

(c) Supplier shall ensure that any persons authorised by it to Process Customer Personal Data are subject to an obligation of confidentiality.

(d) Supplier shall implement appropriate technical and organisational measures to ensure that Customer Personal Data is subject to a level of security appropriate to the risks arising from its Processing by Supplier or its sub-processors, taking into account the factors and measures stated in Article 32 of the GDPR.

(e) Supplier shall notify Customer without undue delay after becoming aware of a Personal Data Breach.

(f) Taking into account the nature of the Processing, Supplier shall assist Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising a Data Subject's rights under Chapter III of the GDPR. For the avoidance of doubt, such assistance may be provided by Supplier providing, as part of the Services, the Customer with functionality to fulfil such requests on a self-service basis and, where Supplier does so, Supplier shall not be obliged to provide any further assistance unless and to the extent that such functionality cannot be used to fulfil the relevant request.

(g) Taking into account the nature of the Processing and the information available to Supplier, Supplier shall assist Customer with regard to Customer's compliance with its obligations under the following Articles of the GDPR:

(i) Article 32 (Security of Processing);

(ii) Articles 33 and 34 (Notification and communication of a Personal Data Breach);

(iii) Article 35 (Data protection impact assessment); and

(iv) Article 36 (Prior consultation by Customer with the Supervisory Authority).

(h) Upon termination of Services that required the Processing of Customer Personal Data (in whole or in part) Supplier shall, at the election of Customer, deliver up or destroy such Customer Personal Data which is in the possession of, or under the control of, Supplier unless European Law requires Supplier to store such Customer Personal Data.

(i) Supplier shall be generally entitled to appoint further processors to process the Customer Personal Data in accordance with clause 2.6.

(j) Supplier shall, at the request of Customer, provide Customer with all information necessary to demonstrate Supplier's compliance with its obligations under this clause 2.3 and, if and to the extent that such provision of information does not demonstrate Supplier's compliance with its obligations under this clause 2.3, Supplier shall allow for and contribute to audits and inspections conducted by or on behalf of Customer subject to the following:

(i) the Customer may perform such audits no more than once per year, save that further audits may be performed if an audit reveals any material non-compliance by us with our obligations in this clause 2.3 (the scope of such further audits being limited to auditing our compliance with those obligations that were not complied with);

(ii) the Customer shall, and shall procure that any third party auditor will, enter into a confidentiality agreement in such form as is reasonably requested by Supplier prior to the conduct of such audit;

(iii) audits must be conducted during regular business hours (i.e. 9am to 5pm UK time) and must not unreasonably interfere with the Supplier's business;

(iv) the Customer must provide the Supplier with any audit reports generated pursuant to any audit at no charge, unless prohibited by applicable law. The Customer shall keep the audit reports confidential and may use the audit reports only for the purposes of meeting its audit requirements under Data Privacy Laws and/or confirming compliance with the requirements of this clause 2.3;

(v) Customer shall, prior to the conduct of an audit, submit an audit plan to the Supplier at least six weeks (or such shorter period as required by law or by a Supervisory Authority) in advance of the proposed commencement date of the audit, setting out the proposed scope, duration and start date of the audit. The Supplier will review the audit plan and will notify the Customer within two weeks of receiving the audit plan if agrees with the plan or if it has any objections in respect of the same. The Supplier will work cooperatively with the Customer to agree a final audit plan;

(vi) nothing in this clause shall require the Supplier to breach any duties of confidentiality owed to any of its clients, employees or other third-parties;

(vii) notwithstanding anything else in this DPA and/or the Agreement, all audits are at the Customer's sole cost and expense.

2.4 **Obligations of Customer**

(a) Without prejudice to the generality of clause 2.2, Customer shall ensure that:

(i) the supply to Supplier of Customer Personal Data by or on behalf of the Customer for the purposes of Processing undertaken by the Supplier and its permitted sub-processors where such Processing is authorised by Customer shall comply with the Data Privacy Laws;

(ii) there is a lawful basis in respect of Supplier's Processing of the Customer Personal Data and Data Subjects have been provided with a privacy policy or notice that complies with the requirements of Article 13/14 of the GDPR in respect of such Processing; and

(iii) the instructions given by Customer to Supplier by operation of clause 2.3(a) shall comply with the Data Privacy Laws.

2.5 **Costs of compliance**

The Customer acknowledges and agrees that the remuneration in respect of the Services takes account of compliance with this DPA and Data Privacy Laws, but does not take into account any additional costs that may be incurred by Supplier in complying with any additional instructions from the Customer outside of those required under this DPA and not required by law. Accordingly, Customer will pay Supplier in respect of any material costs that are (or are to be) reasonably incurred by Supplier outside its compliance with the applicable Data Privacy Laws in respect of the performance by Supplier of such additional instructions, except where such performance is required as a result of a breach by Supplier of its obligations under this DPA or to comply with Data Privacy Laws. Where practicable to do so, Supplier will seek Customer's written approval prior to incurring such costs.

2.6 **Supplier's appointment of sub-processors**

(a) Notwithstanding any other provision of the Agreement (including this DPA), Supplier shall be entitled to appoint further Processors to Process the Processing of Customer Personal Data ("**Sub-processor**"). The following apply in respect of the appointment of Sub-processors:

(i) the Customer approves the appointment of the Sub-processor's identified in Schedule 2;

(ii) Supplier shall notify Customer in writing of its intention to engage any additional Sub-processor. Such notice shall give details of the identity of such Sub-processor and the services to be supplied by it;

(iii) the Supplier shall only use a Sub-processor that has provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Privacy Laws and ensures the protection of the rights of data subjects;

(iv) the Supplier shall impose, through a legally binding contract between the Supplier and the Sub-processor, data protection obligations on the Sub-processor that are in all material respects equivalent to those set out in this DPA and which in any event meet the requirements set out in the Data Privacy Laws;

(v) the Customer shall be entitled to object to the appointment of the Sub-processor where it considers that such appointment will not comply with the requirements of this clause 2.6. Customer shall be deemed to have approved the engagement of the Sub-processor if it has not served a notice in writing on Supplier objecting (in accordance with this clause 2.6(a)(v)) to such appointment within

seven days of the date that the notice is deemed to be received by Customer in accordance with clause 2.6(a)(ii);

(vi) where the Customer objects to the proposed appointment, the Supplier will use commercially reasonable efforts to provide the Services without the use of the relevant Sub-processor. Where the Supplier is unable to provide the Services notwithstanding its use of such commercially reasonable efforts, the Supplier shall have no liability for any failure to provide the relevant Services in accordance with the Agreement; and

(vii) the Supplier shall remain fully liable for all acts or omissions of the Sub-processors as if they were acts or omissions of the Supplier.

2.7 **Restricted Transfers**

(a) The parties acknowledge and agree that the transfer of Customer Personal Data from one party (or its Affiliate(s) to the other party (or its Affiliate(s) is not:

(i) a Restricted Transfer; or

(ii) made on the basis of an Adequacy Framework.

(b) If and to the extent that the transfer of Customer Personal Data becomes subject to a Restricted Transfer or one or more Adequacy Frameworks, the parties shall enter into a separate addendum to implement a Relevant Transfer Mechanism or to give contractual effect to the relevant Adequacy Frameworks.

(c) Customer acknowledges and agrees that Customer Personal Data may be transferred by Supplier to Sub-processors located in a Restricted Country, which may be considered a Restricted Transfer. In the event of the transfer being considered a Restricted Transfer, the Supplier shall enter into a transfer mechanism to ensure that the Restricted Transfer meets the International Transfer Requirements, and Supplier shall provide details of the relevant transfer mechanism on request or as set out in Schedule 2.

2.8 **Losses / Liability**

(a) Where, in accordance with the provisions Article 82 of the GDPR, both parties are responsible for the act, or omission to act, resulting in the payment of Losses by a party, or both parties, then each party shall only be liable for that part of such Losses which is in proportion to its respective responsibility.

(b) Each party's liability under or in connection with this DPA shall be limited in accordance with the liability and limitation provisions of the Agreement.

3 GENERAL

This DPA constitutes the entire agreement and understanding between the parties in respect of the matters set out in this DPA and supersedes any previous agreement or any other part of the Agreement between the parties in relation to such matters.

SCHEDULE 1

Data Processing Details

Subject matter of processing:	The context for the processing of Customer Personal Data is the Supplier's provision of the Services under the Agreement, which shall involve performance on behalf of Customer of the tasks and activities set out in the Agreement for the purpose of providing those Services.
Duration of the processing:	The period for which the Supplier will be providing the Services to the Customer.
Nature and purpose of the processing:	The Supplier may be required to access, receive, generate, store or otherwise process Customer Personal Data in order to provide the Services.
Categories of data subject:	Authorised users of the Service
Type of personal data:	Name, e-mail address and mobile phone number
Location of processing by Supplier:	UK save as set out below

SCHEDULE 2

List of sub-processors

Permitted Sub-processors and location of processing

Name	**Services**	**Location**	**Relevant Transfer Mechanism / Adequacy Framework (if applicable)**
Intercom Software UK Ltd, Level 9, the Warehouse 207-211 Old St, London, EC1V 9NR, United Kingdom	Live-chat & event-based emails.	United States	Standard Contractual Clauses (as defined in Intercom DPA)
HubSpot, 2 Canal Park Cambridge, MA 02141 United States	Customer Relationship Management and Email enrichment services (Clearbit)	United States	Standard Contractual Clauses (as defined in Hubspot DPA)
Zapier, Zapier, Inc., 548 Market St. #62411, San Francisco, CA 94104-5401, United States	Inter-platform Data Synchronisation	United States	Standard Contractual Clauses (as defined in Zapier DPA)
Slack Technologies Limited, Salesforce Tower 60 R801, North Dock Dublin, Ireland	Internal Event Alerting	United States	Standard Contractual Clauses (as defined in Slack Privacy Policy)

SendGrid c/o Twilio UK Ltd, 280 Bishopsgate, London, EC2M 4RB, United Kingdom	Transactional Emails	United States	Standard Contractual Clauses (as defined in Sendgrid Privacy Policy)
Google UK Ltd, Belgrave House, 76 Buckingham Palace Road, London, SW1W 9TQ, United Kingdom	Cloud Hosting Services	United Kingdom	
Chartmogul GmbH & Co. KG, c/o WeWork, Kemperplatz 1, 10785 Berlin, Germany	Revenue Analytics	EU	
Fivetran UK Ltd, Suite 2 First Floor, 10 Temple Back, Bristol, BS1 6FL, United Kingdom	Data processor	EU	
Jiminny Ltd, 100 Fenchurch Street, Second Floor, London, EC3M 5JD, United Kingdom	Call recording	United States of America, Ireland, the United Kingdom and other locations	Standard Contractual Clauses (as defined in https://jiminny.com/dpa)
Posthog, registered in UK as Hiberly Ltd, 18a King Street, Maidenhead, Berkshire, SL6 1EF, United Kingdom	Product analytics	EU	
Stripe, 7th Floor, The Bower Warehouse, 211 Old Street, London, EC1V 9NR, United Kingdom	Card payment provider	United States and Ireland	Standard Contractual Clauses (as defined in https://stripe.com/gb/privacy)
Count Technologies Ltd, Finsgate, 5-7 Cranwood Street, London, EC1V 9EE, United Kingdom	Data analysis platform	United Kingdom	
Elasticsearch B.V. Attn: Privacy	Log recording and processing	United Kingdom (hosted in Intruder	

Team Keizersgracht 281 1016 ED Amsterdam The Netherlands		Google Cloud infrastructure)	
Xero (UK) Limited 5th Floor, 100 Avebury Boulevard, Milton Keynes, MK9 1FH, United Kingdom	Accounting software	United Kingdom	
Lunos Inc., 447 Broadway, 2nd Floor Unit 273, New York, NY 10013, United States	Automated accounts payable	United States	Standard Contractual Clauses (as defined in https://app.lunos.ai/privacy)
Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, California 94104-5401, USA	AI provider	United States	Standard Contractual Clauses (as defined in https://privacy.claude.com/en/articles/10458704-how-does-anthropic-protect-the-personal-data-of-claude-users)