perimeter 81

Data Protection Addendum

This Data Protection Addendum ("**Addendum**") forms an integral part of the Terms of Service (the "**Agreement**") by and between Perimeter 81 Ltd. or any of its affiliates ("**Perimeter 81**") and you, whether you are an existing customer who accepted the Agreement or a new customer accepting the Agreement now ("**Customer**"). Each of Perimeter 81 and Customer may be referred to herein as a "**Party**" and collectively the "**Parties**".

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. The exhibits, annexes, appendices and schedules attached to this Addendum (each an "**Annex**") form an integral part hereof and are expressly incorporated herein by this reference.

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 Addendum to the Agreement are to the Agreement as supplemented by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulation.

1.1.2 "**Customer Personal Data**" means any Personal Data or Personal Information Processed by Perimeter 81 on behalf of Customer pursuant to or in connection with the Agreement;

1.1.3 "**EEA**" means the European Economic Area;

1.1.4 "**GDPR**" means EU General Data Protection Regulation 2016/679

1.1.5 "**Services**" means the Service and any other activities to be supplied to or carried out by or on behalf of Perimeter 81 for Customer pursuant to the Agreement;

1.1.6 "**Standard Contractual Clauses**" means the Standard Contractual Clauses attached as Annex 3 hereto. Should any subsequent version thereof be released by the European Commission, Annex 3 shall be amended accordingly;

1.1.7 "**Subprocessor**" means any person (including any third party, but excluding an employee of Perimeter 81 or any of its affiliates) appointed by or on behalf of Perimeter 81 to Process Personal Data in connection with the Agreement. The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "Process" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. The term "**Personal Information**" shall have the same meaning as in the CCPA.

perimeter 81

1.2 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 Perimeter 81 will Process Customer Personal Data as a Processor, in accordance with Customer's documented instructions, unless Processing is required by applicable laws to which Perimeter 81 is subject, in which case Perimeter 81 will, to the extent permitted by applicable laws, inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.2 Customer hereby:

2.2.1 instructs Perimeter 81 to Process Customer Personal Data (including, by transferring Customer Personal Data to any country or territory) as reasonably necessary for the provision of the Services and in accordance with this Addendum; and

2.2.2 warrants and represents that it is and will at all relevant times remain (a) duly and effectively authorized to give the instruction set out in section 2.2.1; (b) the Controller of the Customer Personal Data Processed by Perimeter 81; and (c) responsible for and in compliance with its obligations as a Controller of Customer Personal Data under applicable law (including the GDPR), in particular with respect to the justification of any Processing of Customer Personal Data by Perimeter 81.

2.3 Perimeter 81 shall not retain, use, or disclose Customer Personal Data (a) for any purpose other than for the specific purpose of performing the Services or as otherwise strictly permitted under the Agreement or this Addendum; or (b) for any commercial purpose, other than for providing the Services; and shall not sell Customer Personal Data. Perimeter 81 hereby certifies that it understands the restrictions under this Section 2.3 and will comply with them.

2.4 Notwithstanding the above, Customer will be solely responsible for: (a) providing any required notices, obtaining and documenting any required consents and/or authorizations to/from Data Subjects and/or other third parties, including obtaining explicit consent to the processing of special categories of data, all in accordance with Articles 7-9 and 12-14 of the GDPR; (b) securing an appropriate legal basis under applicable law, as necessary for Perimeter 81 to Process Customer Personal Data as a Processor on Customer's behalf (including Processing under Annex 3 where applicable); (c) ensuring that Company Personal Data is accurate and up to date; and (d) Customer's decisions and actions concerning the Processing of such Customer Personal Data.

3. Annex 1

to this Addendum sets out certain information regarding the Processing of the Customer Personal Data by Perimeter 81 and/or any Subprocessors as required by Article 28(3) of the GDPR. Nothing in **Annex 1** confers any right or imposes any obligation on any Party to this Addendum.

perimeter 81

4. Perimeter 81 Personnel

Perimeter 81 will ensure that Perimeter 81 employees authorized to process Customer Personal Data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

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, Perimeter 81 will in relation to the Customer 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. Customer is solely responsible for implementing appropriate internal measures for securing Customer Personal Data held and/or Processed by the Customer, including in connection with Customer's use of the Services, and for the secure transfer of Customer Personal Data to Perimeter 81.

6. Subprocessing

6.1 Customer authorizes Perimeter 81 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 Perimeter 81 may continue to use those Subprocessors already engaged by it at the date of this Addendum, as listed in **Annex 2**.

6.3 Customer authorizes Perimeter 81 to use additional Subprocessors, provided that Perimeter 81 will notify Customer of the addition of any Subprocessor and give the Customer an opportunity to object in writing thereto, within fourteen (14) days of receiving such notice.

6.4 With respect to each Subprocessor, Perimeter 81 will ensure that such Subprocessor is required by written contract to abide by the same level of data protection and security as Perimeter 81 under this Addendum, as applicable to such Subprocessor's Processing of Customer Personal Data.

7. International Transfer of Personal Data

7.1 Perimeter 81 is allowed (and allowed to authorize its Subprocessors) to transfer Customer Personal Data outside of the EEA and UK (including cloud storage in the United States) in the following cases: (a) Customer Personal Data is transferred to a country or scheme which is approved by the European Commission as ensuring an adequate level of protection ("**Approved Jurisdictions**"); (b) subject to the entry into the Standard Contractual Clauses by the transferor and the transferee with respect to the transfer of Customer Personal Data; or (c) if the transfer falls within a permitted derogation.

7.2 To the extent that Perimeter 81 Processes Personal Data outside of the EEA and UK and/or Approved Jurisdictions, then the Parties shall be deemed to enter into the Standard Contractual Clauses, in which event the Customer shall be deemed as the data exporter and Perimeter 81 shall be deemed as the data importer (as these terms are defined therein);

perimeter 81

8. Data Subject Rights

Taking into account the nature of the Processing, Perimeter 81 will provide reasonable assistance to Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to requests to exercise Data Subject rights under the GDPR.

9. Personal Data Breach

Perimeter 81 will notify Customer upon Perimeter 81 becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer, to the extent reasonable, with sufficient information to allow Customer to meet its obligations to report or inform Data Subjects of the Personal Data Breach.

10. Data Protection Impact Assessment and Prior Consultation

Perimeter 81 will, at Customer's expense, provide reasonable assistance to Customer with data protection impact assessments, and prior consultations with Supervisory Authorities, which Customer reasonably considers to be required by Article 35 or 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by Perimeter 81, and taking into account the nature of the Processing and information available to Perimeter 81.

11. Deletion of Customer Personal Data

11.1 Without derogating from the Agreement, at the choice of the Customer all Customer Personal Data are to be deleted or returned to the Customer after the end of the provision of Services.

11.2 Notwithstanding Section 11.1, Perimeter 81 may retain Customer Personal Data to the extent and for such period as required by a subpoena or other judicial or administrative order, or if otherwise required by law. Perimeter 81 will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its retention and for no other purpose.

12. Provision of Information Demonstrating Compliance and Audits

Upon Customer's request up to once per year, Perimeter 81 shall make available to Customer evidence that Perimeter 81 is in compliance with this Addendum. Perimeter 81 and Customer agree that such demonstration of compliance by Perimeter 81 is the preferred mechanism for meeting the requirements of article 28(3)(h) of the GDPR. Audit requirements shall be met upon Perimeter 81's provision, provided that the parties have an applicable confidentiality agreement in place, of third party certification (which may include the then-current SOC2 report). Any request for additional audit rights shall be at Customer's expense and Perimeter 81' sole discretion.

13. General Terms

Disclosure to competent authorities

13.1 To the extent required by applicable law, Perimeter 81 may disclose Customer Personal Data if required by a subpoena or other judicial or administrative order, or if otherwise required by law, provided that Perimeter 81 will, prior to such disclosure and to the extent permitted by applicable law, notify Customer and provide Customer an opportunity to object to such disclosure.

Severance

13.2 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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.

13.3 This Addendum may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. In the event that a Party's signature is delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of such Party with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.

ANNEX 1
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data pursuant to Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter of the Processing of Customer Personal Data is set out in the Agreement and the duration thereof is for the term of the Agreement.

The nature and purpose of the Processing of Customer Personal Data

Perimeter 81 may Process Customer Personal Data for the purpose of providing the Services to the Customer, including: (i) providing maintenance services and technical and other support with respect to the Services; (ii) cloud storage services; (iii) analysis; (iv) complying with Customer's documented written instructions; or (v) complying with applicable law; or (vi) for users of web security features – monitoring and/or collection of data regarding web browsing activity, including encrypted pages (e.g., SSL). In addition, Perimeter 81 may process aggregated and/or anonymized Customer Personal Data to maintain and improve the Services and the technology used therefor.

The types of Customer Personal Data to be Processed

Customer Personal Data typically includes name and work-related Personal Data, such as email address, IP address, device information, web browsing data and contact details.

The categories of Data Subjects to whom the Customer Personal Data relates

Customer personnel.

The obligations and rights of the parties

The obligations and rights of the Controller and Processor are set out in this Addendum.

perimeter 81

ANNEX 2
AUTHORIZED SUB-PROCESSORS

SUB-PROCESSOR NAME	PURPOSE OF PROCESSING	ENTITY COUNTRY	TYPE OF DATA PROCESSED
Amazon Web Services, Inc.	Cloud Service Provider	United States	All data specified in Annex I
MongoDB Atlas	Cloud Service Provider	United States	All data specified in Annex I
SendGrid, Inc.	Database connection	United States	All data specified in Annex I
SFDC	CRM services	United States	All data specified in Annex I
G-Suite (Google Workspace)	Email and Cloud services	Ireland	All data specified in Annex I
Looker Data Sciences	BI services	United States	All data specified in Annex I
Marketo Inc.	Marketing database	Ireland	All data specified in Annex I
Intercom Inc.	Online chat services	United States	All data specified in Annex I
Calendly LLC.	Calendar services	United States	All data specified in Annex I
Chargebee	Billing and collection services	United States	All data specified in Annex I
Delighted	Satisfaction Surveys (NPS)	United States	All data specified in Annex I
Freshworks	Support System	United States	All data specified in Annex I
Drift Email	Marketo emails response routing	United States	All data specified in Annex I
Chili piper	Calendar services	United States	All data specified in Annex I
Clearbit	Lead Enrichment tool	United States	All data specified in Annex I All data specified in Annex I
Alyce	Lead Engagement tool	United States	All data specified in Annex I
SalesLoft	Lead Engagement Platform	United States	All data specified in Annex I
Lusha	Lead Enrichment tool	United States	All data specified in Annex I
TryProspect	Lead Enrichment tool	Canada	All data specified in Annex I
Orum	Lead Engagement tool	United States	All data specified in Annex I
Allbound	Partner Portal Platform	United States	All data specified in Annex I

perimeter 81

ANNEX 3
EU STANDARD CONTRACTUAL CLAUSES (MODULE 2)

Section 1

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

perimeter 81

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

[Intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

perimeter 81

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or**(iv)** Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are

indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least fourteen (14) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) he specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

perimeter 81

ANNEX 1

A. LIST OF PARTIES

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: As described in Annex 1 of the DPA – Details of the processing.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

Name: Perimeter 81 Ltd.

Address: 28 Ha'Arbaa St, Tel Aviv, Israel.

Contact person's name, position and contact details: VP of Finance, Legal@perimeter81.com

Activities relevant to the data transferred under these Clauses: As described in Annex 1 of the DPA – Details of the processing.

Signature and date:

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: as described in Annex 1 of the DPA – Details of the processing.

Categories of personal data transferred: as described in Annex 1 of the DPA – Details of the processing.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: as described in Annex 1 of the DPA – Details of the processing.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): as described in Annex 1 of the DPA – Details of the processing.

Nature of the processing: as described in Annex 1 of the DPA – Details of the processing.

Purpose(s) of the data transfer and further processing: as described in Annex 1 of the DPA – Details of the processing.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: as described in Annex 1 of the DPA – Details of the processing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: as described in Annex 1 of the DPA – Details of the processing.

C. COMPETENT SUPERVISORY AUTHORITY

As set forth in Clause 13 above.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Perimeter 81 implements administrative, contractual, and technical procedures to protect the Personal Data it processes.

Perimeter 81 has ISO27001 and SOC 2 Type II compliance certificates, which can be provided upon request.

Perimeter 81 engages Amazon Web Services (AWS) as a cloud service provider for hosting its server-side infrastructure and certain data in rest. Perimeter 81's data in rest is also stored on MongoDB Atlas.

Perimeter 81 is registered for AWS Business Support which includes 24x7 support and SLA response time for production incidents of less than one hour. Additional information can be found here: https://aws.amazon.com/premiumsupport/plans/. Along with AWS support, our DevOps engineers are available 24x7 and our AWS systems infrastructure is fully monitored by PagerDuty.

Perimeter 81 uses load balancers and a web application firewall (WAF) to prevent unauthorized access through the internet. Components that process Personal Data only operate in Perimeter 81's private network inside our secure cloud platform.

Perimeter 81 encrypts all data transfers between itself and its contractors or clients with up-to-date encryption protocols, including TLS 1.2 and mTLS. Perimeter 81 also utilizes AWS Key Management Services (KMS) and restricts access to the cryptographic keys to limited authorized personnel only.

Perimeter 81's internal services that manage Perimeter 81's platform are available only via a virtual private network, with the exception of services that must have access to the public internet. Access to the internal services is logged and monitored.

Only a limited number of authorized personnel may access Personal Data, on a need-to-know basis, and through a leading top industry-standard IDP management system that utilizes complex passwords, multi-factor authentication, and personalized user accounts.

Perimeter 81's Compliance Team defines and controls the collection, processing, and storage of customers' Personal Data.

ANNEX III – LIST OF SUB-PROCESSORS

As detailed in Annex 2 of the DPA.