perimeter 81

Data Processing Agreement/Addendum

This Data Processing Agreement **("DPA")** forms part of our Terms of Service **("Agreement")** whether you are an existing customer who accepted the Agreement or a new customer accepting the Agreement now. You acknowledge that you, on your own behalf as an individual and on behalf of your employer or another legal entity (collectively, **"you", "your", "Customer", or "Data Controller", "The Organization"**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with Perimeter 81 LTD. the owner of perimeter81.com **("perimeter81.com", "us", "we", "our", "service provider" or "Data Processor")** to reflect the parties' agreement with regard to the Processing of Personal Data of European individuals who benefit from the protection of the GDPR. Both parties shall be referred to as the "Parties" and each, a "Party".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

You represent and warrant that you have, or you were granted, full authority to bind the Organization to this DPA. If you cannot, or do not agree to, comply with, and be bound by, this DPA or do not have authority to bind the Organization or any other entity, please do not supply or provide Personal Data to us.

You enter into this DPA on behalf of yourself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of the Organization and the Organization's Authorized Affiliates, if and to the extent that you or the Organization processes Personal Data for which such Authorized Affiliates qualify as the "data controller". For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include yourself, the Organization and/or the Organization's Authorized Affiliates.

In the course of providing the Services pursuant to the Agreement, we may process Personal Data on your behalf, in the capacity of a "Data Processor". The Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

If you need a signed copy of this DPA, you can download this agreement at **http://www.perimeter81.com/legal/dpa,** send a signed copy to **legal@perimeter.com** and we'll provide you a countersigned copy.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement.

1. Interpretation and definitions

1.1. The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.

1.2. References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3. Words used in the singular include the plural and vice versa, as the context may require.

1.4. Definitions:

    (a) "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

    (b) "Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws And Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Perimeter 81 LTD., but has not signed its own agreement with Perimeter 81 LTD. and is not a "Customer" as defined under the Agreement.

    (c) "Controller" or "Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

    (d) "Member State" means a country that belongs to the European Union and/or the European Economic Area. "Union" means the European Union.

    (e) "Perimeter 81 LTD" means Perimeter81.com and its Affiliates engaged in the Processing of Personal Data.

(f) "Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

(g) "Data Subject" means the identified or identifiable person to whom the Personal Data relates.

(h) "GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(i) "Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(j) "Process(ing)" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) "Processor" or "Data Processor" means the entity which Processes Personal Data on behalf of the Controller.

(l) "Privacy Documentation" means the Privacy Documentation applicable to the specific. Services purchased by Customer, as updated from time to time, and accessible via **www.perimeter81.com/legal/privacy**, or as otherwise made reasonably available by Perimeter 81 LTD.

(m) "Sub-processor" means any Processor engaged by Perimeter 81 LTD.

(n) "Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2.Processing Of Personal Data

2.1. Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Customer is the Data Controller, (ii) Perimeter 81 LTD. is the Data Processor and that (iii) Perimeter 81 LTD. or members of the Perimeter 81 LTD. Group may engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, 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 means by which Customer acquired Personal Data. Without limitation, Customer shall have any and all required legal bases in order to collect, Process and transfer to Data Processor the Personal Data and to authorize the Processing by Data Processor of the Personal Data which is authorized in this DPA. Customer will be fully responsible for the actions and omissions of its Authorized Users and their use of the Service.

2.3. Data Processor's Processing of Personal Data. Subject to the Agreement with Customer, Data Processor shall Process Personal Data in accordance with Customer's documented instructions regarding the manner in which the Data Processor will process the Personal Data, for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer to be able to use the Services; (iii) Processing to comply with other Personal Data related requests provided by Customer where such requests are consistent with the terms of the Agreement; (iv) Processing as required by Union or Member State law to which Data Processor is subject; in such a case, Data Processor shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

To the extent that Data Processor cannot comply with a request from Customer and/or its Authorized Users (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind), Data Processor (i) shall inform Customer, providing relevant details of the problem, (ii) Data Processor may, without any kind of liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing those data) and/or suspend access to the Account, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Data Processor all the amounts owed to Data Processor or due before the date of termination. Customer will have no further claims against Data Processor (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and the DPA in the situation described in this paragraph.

2.4. Details of the Processing. The subject-matter of Processing of Personal Data by Data Processor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. Rights of Data Subjects

3.1. Data Subject Request. Data Processor shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to access, correct or delete that person's Personal Data or if a Data Subject objects to the Processing thereof ("Data Subject Request"). Data Processor may respond to a Data Subject Request without Customer's consent in order to confirm that such request relates to Customer, to which Customer hereby agrees.

3.2. Data Subject Request. With effect from 25 May 2018, the following wording will replace Section 3.1 ("Data Subject Request") in its entirety: Data Subject Requests. Data Processor shall, to the extent legally permitted, promptly notify Customer if Data Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Data Processor shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Data Processor shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Data Processor is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. Customer shall be responsible for any costs arising from Data Processor's provision of such assistance.

4. Perimeter 81 LTD. Personnel

4.1 Confidentiality. Data Processor shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality.

4.2 Data Processor may disclose and Process the Personal Data (a) to the extent required by a court of competent jurisdiction or other Supervisory Authority, or (b) otherwise as required by applicable Data Protection Laws and Regulations (in such a case, Data Processor shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. Authorization Regarding Sub-Processors

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that (a) Data Processor's Affiliates may be retained as Sub-processors; and (b) Data Processor and Data Processor's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

5.2. List of Current Sub-processors and Notification of New Sub-processors.

5.2.1. By or around May 25, 2018, Data Processor shall make available to Customer the current list of Sub-processors used by Data Processor to process Personal Data via **http://www.perimeter81.com/legal/subprocessors**. Such Sub-processor list shall include the identities of those Sub-processors and their country of location (**"Sub-Processor List"**). The Sub-Processor List as of the date of publication is hereby authorized, and in any event shall be deemed authorized, by Customer unless it provides a written reasonable objection , for reasons relating to the protection of Personal Data, within ten (10) business days following the publication of the Sub -Processor List. Customer may reasonably object to Data Processor's use of an existing Sub-processor by providing a written objection to legal@perimeter81.com. In the event Customer reasonabl y objects to an exi st i ng Sub-processor, as permitted in the preceding sentences, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Customer will have no further claims against Data Processor due to (i) past use of approved Sub-processors prior to the date of objection or
(ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.2.2. By or around May 25, 2018, Customer may find on Data Processor's webpage accessible via **http://www.perimeter81.com/legal/subprocessors** a mechanism to subscribe to notifications of new Sub-processors used to Process Personal Data , to which Customer shall subscribe, and if Customer subscribes, Data Processor shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3. Objection Right for New Sub-processors. Customer may reasonably object to Data Processor's use of a new Sub-processor, for reasons relating to the protection of Personal Data, by notifying Data Processor promptly in writing within three (3) business days after receipt of Data Processor's notice in accordance with the mechanism set out in Section 5.2.2 and such written objection shall include the reasons, relating to the protection of Personal Data, for objecting to Data Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within three (3) business days following Data Processor's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer r eas o n ab l y objects to a new Sub-processor, as permitted in the preceding sentences, Data Processor will use reasonable efforts to make available

to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement an d this DP A with respect only to those Services which cannot be provided by Data Processor without the use of the objected-to new Sub-processor by providing written notice to Data Processor provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Data Processor. Until a decision is made regarding the new Sub-processor, Data Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Account. Customer will have no further claims against Data Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4. Agreements with Sub-processors. Data Processor or a Data Processor's Affiliate has entered into, or shall enter into by May 25, 2018, a written agreement with each Sub-processor containing appropriate

safe guards to the protection of Personal Data. Where Data Processor engages a new Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where the new Sub-processor fails to fulfil its data protection obligations, Data Processor shall remain fully liable to the Customer for the performance of the new Sub-processor's obligations. In accordance with Articles 28.7 and 28.8 of the GDPR, if and when the European Commission lays down the standard contractual clauses referred to in such Articles, the Parties may revise this DPA in good faith to adjust it to such standard contractual clauses.

6. Security

6.1. Controls for the Protection of Personal Data. Data Processor shall maintain industry-standard technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Privacy Documentation which are hereby approved by Customer. Data Processor regularly monitors compliance with these measures. With effect from 25 May 2018, upon the Customer's request, Data Processor will assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Data Processor.

6.2. Third-Party Certifications and Audits. Upon Customer's 14 days prior written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Data Processor shall make available to Customer that is not a competitor of Data Processor (or Customer's independent, reputable, third-party auditor that is not a competitor of Data Processor and not in conflict with Data Processor, subject to their confidentiality and non-compete undertakings) all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Data Processor's prior written approval and, upon Data Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Data Processor in the context of the audit and/or the inspection). Customer shall be fully responsible for bearing all the costs and expenses arising from or related to this Section.

6.3. Further details are provided in the Privacy Documentation.

7. Personal Data Incident Management and Notification Security

Data Processor maintains security incident management policies and procedures specified in Privacy Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Data Processor or its Sub-processors of which Data Processor becomes aware (a "Personal Data Incident"). Data Processor shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Data Processor deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Data Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users and/or their instructions.

8. Return and Deletion of Personal Data

Subject to the Agreement, upon termination of the Agreement, Data Processor shall, at the choice of Customer, delete or return all the Personal Data to Customer in the manner described in the Agreement, and Data Processor shall delete existing copies of the Personal Data unless Data Protection Laws and Regulations require the storage of the Personal Data. Notwithstanding the above, Data Processor may pseudonymize Personal Data, and may then retain pseudonymized data indefinitely. In any event, to the extent allowed or required by applicable law, Data Processor may also retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

9. Authorized Affiliates

9.1. Contractual Relationship. The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates in which case each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

9.2. Communication. The Customer shall remain responsible for coordinating all communication with Data Processor under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10. Other Provisions

10.1. GDPR. With effect from 25 May 2018, the Parties will Process the Personal Data in accordance with the GDPR requirements directly applicable to each Party in the context of the provision and use of the Services.

10.2. Data Protection Impact Assessment. With effect from 25 May 2018, upon Customer's request, Data Processor shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Data Processor. Data Processor shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 10.2 of this DPA, to the extent required under the GDPR.

10.3. Transfer mechanisms for data transfers between the Parties and, if applicable, Authorized Affiliates.

(a)Transfers to countries that offer adequate level or data protection: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, **"EEA"**) to countries that offer adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("Adequacy Decisions"), without any further safeguard being necessary.

(b) Transfers of Personal Data to the United States: The entity of Data Processor established in the United States self-certified to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce, and Data Processor shall comply with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to the Processing of Personal Data that is transferred from the EEA and/or Switzerland to the United States.

(c) Transfers to other countries: If the Processing of Personal Data includes transfers from the EEA to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision **("Other Countries")**, the Parties shall comply, upon Customer's request, with Article 46 of the GDPR, and shall execute the standard data protection clauses adopted by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission or comply with any of the other mechanisms provided for in the GDPR for transferring Personal Data to such Other Countries.

11. Assistance

Data Processor may assist Customer, at Customer's cost, in ensuring compliance with Customer's obligations pursuant to the GDPR.

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER:

Signature:
Customer Name:
Print Name:
Title:
Date:

Perimeter 81 LTD.:

Signature:
Print Name:
Title:
Date:

Schedule 1 - Details of the Processing

Subject matter

Data Processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.

Nature and Purpose of Processing

1. Providing the Service(s) to Customer.

2. Setting up an account/account(s) for Customer.

3. Setting up profile(s) for users authorized by Customer.

4. For Customer to be able to use the Services.

5. For Data Processor to comply with requests provided by Customer where such requests are consistent with the terms of the Agreement.

6. Performing the Agreement, this DPA and/or other contracts executed by the Parties.

7. Providing support and technical maintenance, if agreed in the Agreement.

8. Resolving disputes.

9. Enforcing the Agreement, this DPA and/or defending Data Processor's rights.

10. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fee payment, account administration, accounting, tax, management, litigation; and

11. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.

12. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Data Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Data Processor may retain non-Personal data, anonymize or pseudonymized data indefinitely.

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: First name, Last name, User name, Address, Phone number, Email address, Title, Photo, User Social Networks ids and online identifiers, Personal Data included in the management of the Customer's Project(s), Payment information including card holder name and email, Business information including account name and any other Personal Data or information that the Customer and/or the Data Subjects decide to provide to the Data Processor.

The Customer and the Data Subjects shall provide the Personal Data to Data Processor by supplying the Personal Data to Data Processor's Service, or by supplying it directly to the Data Processor's other channels. In some limited circumstances Personal Data may also come from other sources, for example, in the case of anti-money laundering research or as required by applicable law. For clarity, Customer shall always be deemed the "Data Controller" and Perimeter 81 LTD. shall always be deemed the "Data Processor" (as such terms are defined in the GDPR).

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- **Customer's users authorized by Customer to use the Services**

- **Employees, agents, advisors, freelancers of Customer (who are natural persons)**

- **Prospects, customers, business partners and vendors of Customer (who are natural persons)**

- **Employees or contact persons of Customer's prospects, customers, business partners and vendors**

- **Any other third party with which Customer decides to communicate through the Service.**