DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1 You and ZenLeads Inc. ("**Company**", "**we**", "**our**" or "**us**") entered into an agreement, comprising the Order and the Agreement, (the "**Agreement**"), for the provision of the Services.

1.2 In the event that we Process any Customer Personal Data (each as defined below) and (i) the Customer Personal Data relates to individuals located in the EEA; or (ii) you are established in the EEA, this Data Processing Addendum (the "**DPA**") shall be supplemental to the Agreement and apply to the Processing of such Customer Personal Data. In the event of a conflict between any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

1.3 This DPA is between you and Company (each a "**Party**" and collectively the "**Parties**").

2. DEFINITONS

2.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement, and the following capitalised terms used in this DPA shall be defined as follows:

(a) "**Controller**" has the meaning given in the GDPR.

(b) "**Customer Personal Data**" means the "**personal data**" (as defined in the GDPR) described in ANNEX 2 and any other personal data contained in the User Data (or any other data) that we process on your behalf in connection with our provision of the Services.

(c) "**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 ("**GDPR**"), any applicable national implementing legislation in each case as amended, replaced or superseded from time to time, and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Customer Personal Data.

(d) "**Data Subject**" has the meaning given in the GDPR.

(e) "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

(f) "**Processing**" has the meaning given in the GDPR, and "**Process**" will be interpreted accordingly.

(g) "**Processor**" has the meaning given in the GDPR.

(h) "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data.

(i) "**Standard Contractual Clauses**" means the Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 set out in ANNEX 1 to this DPA or any subsequent version thereof released by the European Commission (which will automatically apply), and which includes ANNEX 2 (Details of the Transfer) and ANNEX 3 (Technical and Organisational Measures) to this DPA.

(j) "**Subprocessor**" means any Processor engaged by us who agrees to receive from us Customer Personal Data.

(k) "**Supervisory Authority**" has the meaning given in the GDPR.

3. DATA PROCESSING

3.1 **Instructions for Data Processing.** We will only Process Customer Personal Data in accordance with your written instructions. The Agreement (subject to any changes to the Services agreed between the Parties) and this DPA shall be your complete and final instructions to us in relation to the processing of Customer Personal Data.

3.2 Processing outside the scope of this DPA or the Agreement will require prior written agreement between you and us on additional instructions for Processing.

3.3 **Required consents.** Where required by applicable Data Protection Laws, you will ensure that you have obtained/will obtain all necessary consents for the Processing of Customer Personal Data by us in accordance with the Agreement.

4. TRANSFER OF PERSONAL DATA

4.1 **Authorized Subprocessors.** You agree that we may use the following as Subprocessors to Process Customer Personal Data: Google Compute Platform, Microsoft Azure

4.2 You agree that we may use subcontractors to fulfil our contractual obligations under the Agreement. We shall notify you from time to time of the identity of any Subprocessors we engage. If you (acting reasonably) object to a new Subprocessor on grounds related to the protection of Customer Personal Data only, then without prejudice to any right to terminate the Agreement, you may request that we move the Customer Personal Data to another Subprocessor and we shall, within a reasonable time following receipt of such request, use reasonable endeavours to ensure that the original Subprocessor does not Process any of the Customer Personal Data. If it is not reasonably possible to use another Subprocessor, and you continue to object for a legitimate reason, either party may terminate the Agreement on thirty (30) days written notice. If you do not object within thirty (30) days of receipt of the notice, you are deemed to have accepted the new Subprocessor.

4.3 Save as set out in clauses 0 and 4.2, we shall not permit, allow or otherwise facilitate Subprocessors to Process Customer Personal Data without your prior written consent and unless we enter into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Customer Personal Data, as are imposed on us under this DPA.

4.4 **Liability of Subprocessors**. We will at all times remain responsible for compliance with our obligations under the DPA and will be liable to you for the acts and omissions of any Subprocessor as if they were our acts and omissions.

4.5 **Prohibition on Transfers of Personal Data**. To the extent that the Processing of Customer Personal Data by us involves the export of such Customer Personal Data to a country or territory outside the EEA, other than a country or territory ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data as determined by the European Commission (an "**International Transfer**"), such transfer shall be governed by the Standard Contractual Clauses. In the event of any conflict between any terms in the Standard Contractual Clauses, this DPA and the Agreement, the Standard Contractual Clauses shall prevail.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 **Company Security Obligations**. 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, we will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the measures set out in ANNEX 3.

5.2 Upon your reasonable request, we will make available all information reasonably necessary to demonstrate compliance with this DPA.

5.3 **Security Incident Notification.** If we or any Subprocessor become aware of a Security Incident we will (a) notify you of the Security Incident within 72 hours, (b) investigate the Security Incident and provide you (and any law enforcement or regulatory official) with reasonable assistance as required to investigate the Security Incident, and (c) take steps to remedy any non-compliance with this DPA.

5.4 **Company Employees and Personnel.** We will treat the Customer Personal Data as the confidential, and shall ensure that any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

5.5 **Audits**. We will, upon your reasonable request, allow for and contribute to audits, including inspections, of our compliance with this DPA, conducted by you (or a third party on your behalf and mandated by you) provided (i) such audits or inspections are not conducted more than once per year (unless requested by a Supervisory Authority); (ii) are conducted only during business hours; and (iii) are conducted in a manner that causes minimal disruption to Company's operations and business.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 **Government Disclosure.** We will notify you of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

6.2 **Data Subject Rights.** Where applicable, and taking into account the nature of the Processing, we will use reasonable endeavors to assist you by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of your obligation to respond to requests for exercising Data Subject rights laid down in the GDPR.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, we will provide you with reasonably requested information regarding our Services to enable you to carry out data protection impact assessments or prior consultations with any Supervisory Authority, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to us.

8. TERMINATION

8.1 **Deletion of data**. Subject to 8.2 below, we will, at your election within 90 (ninety) days of the date of termination of the Agreement:

(a) delete and use all reasonable efforts to procure the deletion of Customer Personal Data Processed by us or any Subprocessors; or

(b) return a complete copy of all Customer Personal Data by secure file transfer in such a format as notified to us by you.

8.2 We and our Subprocessors may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that we ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

ANNEX 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of this ANNEX 1, references to the "data exporter" and "data importer" shall be to you and to Company respectively (each a "*party*"; together "*the parties*").

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex 2 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex 3 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 3, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex 3 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 3 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated as needed. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

ANNEX 2

DETAILS OF THE TRANSFER FORMING PART OF THE STANDARD CONTRACTUAL CLAUSES

Data exporter

You are the data exporter.

Data importer

The data importer is Company.

Data subjects

The data exporter may submit Customer Personal Data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to prospects, customers, business partners and vendors of data exporter

Categories of data

Data exporter may submit Customer Personal Data, the extent of which is determined and controlled by the data exporter, and which may include, but is not limited to the following categories of Customer Personal Data:

- First and last name
- Title
- Employer
- Contact information (company, email, phone, physical business address)

Processing operations

The objective of process of Customer Personal Data by data importer is provision of services to the data exporter pursuant to the Agreement between date exporter and data importer.

ANNEX 3

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES FORMING PART OF THE STANDARD CONTRACTUAL CLAUSES

Company currently observes the security practices described in this Appendix 3. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, Company may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Company Customer Terms of Service.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Company hosts its Service with outsourced, US-based data center providers. Additionally, Company maintains contractual relationships with vendors in order to provide the Service. Company relies on contractual agreements, privacy policies, and vendor compliance programs in order to assure the protection of data processed or stored by these vendors.

Physical and environmental security: Company hosts its product infrastructure with multi-tenant, outsourced data center providers. The physical and environmental security controls are audited for SOC 2 Type I compliance.

Authentication: Company implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Company's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

Company implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure.

Static code analysis: Security reviews of code stored in Company's source code repositories is performed, checking for coding best practices and identifiable software flaws.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Company's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

b) Transmission Control

In-transit: Company makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Company products. Company's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Company stores user passwords following policies that follow at least industry standard practices for security.

c) Input Control

Detection: Company designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Company personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Company maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Company will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Company becomes aware of unlawful access to Customer data stored within its products, Company will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Company is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Company deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Company selects, which may include via email or telephone.

d) Job Control

The Company Product provides a solution for Customers to conduct their marketing and sales activities. Customers control the data types collected by and stored within their portals. Company never sells personal data to any third party.

Terminating Customers: Customer Data in active (i.e., primary) databases is purged upon a customer's written request, or for our web-based application available at https://www.Company.com, 90 days after a customer terminates all agreements for such products with Company. Marketing information stored in backups, replicas, and snapshots is not automatically purged, but instead ages out of the system as part of the data lifecycle. Company reserves the right to alter data purging period in order to address technical, compliance, or statutory requirements.

e) Availability Control

Infrastructure availability: The data center providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple data centers and availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Company's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Company operations in maintaining and updating the product applications and backend while limiting downtime.

f) Separation in Processing

Company's collection of personal data from its Customers is to provide and improve our products. Company does not use that data for other purposes that would require separate processing.