eLama Global Data Processing Terms and Conditions

With this document Elama Global PTE LTD. (the "**DPS Provider**", "**eLama**") and the counterparty (the "**Customer**") to the below outlined and accept the terms for provision of the Data Processor Services (further the "**DPS Agreement**"/ "**Agreement**") between the parties.

This DPS Agreement determines the terms and conditions of Data Processing and security standards in connection to European and Brazil Data Protection legislation. This DPS Agreement supplement all other Data Processing and Service Provision Agreements between eLama Global PTE LTD. and their customers. This DPS Agreement will be effective for all the territories, in which the DPS Provider or the Customer is present.

By accepting this DPS Agreement on behalf of the Customer you confirm that:

- you have full legal authority to bind the Customer to the terms of data processing and operation, outlined further in this Agreement;
- You have read and understood the terms, outlined in this Agreement;
- You agree on behalf of the Customer to enter in agreement on terms and conditions of this Agreement.

If you do not have legal authority or do not fully agree with the terms and conditions, outlined in this Agreement, please do not accept it.

1. Interpretation and Definition of terms

1.1. Terms used in this DPS:

eLama Service is a system of automated management of Advertising Campaigns on the Internet, located at eLama branded websites, through which the Customer can post Advertising Materials to Online Advertising Platforms on its own behalf or on behalf of its clients as well as receive other services.

Supplementary Service means a product, service or application provided by eLama or a third party that: (a) is not part of the eLama Services; and (b) is accessible for use within the user interface of the Processor Services or is otherwise integrated with the eLama Services.

Affiliate entity refers to an entity (subcontroller, subprocessor) that directly or indirectly controls, is controlled by, or is under common control with, one of the parties to this Agreement.

Third party entity refers to an entity that does not have direct or indirect control or common control and is not controlled by any of the parties to this Agreement.

Customer Personal Data refers to personal data of individuals or legal entities that is provided to the DPS Provider by the Customer and thus is processed by any of the parties to this Agreement.

Data Incident refers to an actual breach of the DPS Provider security standards (as described in clause 5 below) or terms of this Agreement, leading to alteration, unauthorised disclosure, use, or access to or accidental or illegal disclosure of Customer Personal Data on systems, directly or indirectly managed or owned by the DPS Provider . This does not include unsuccessful attempts

of unlawful or accidental actions that do not result in actual breach of security and disclosure, alteration or access to Customer Personal Data.

Data Protection Legislation refers to, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) and (c) Lei Geral de Proteção de Dados (LGPD) lei 13.709/18 from 13 August 2018 (Brazil).

EEA refers to the European Economic Area.

GDPR refers to 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.

Notification Email Address refers to the email address (if any) informed by the Customer, via the user interface of the DPS Provider or such other means provided by the DPS Provider, to receive certain notifications from the DPS Provider, relating to these Data Processing Terms.

Subprocessors refers to the third parties authorised under these Data Processing Terms and Conditions to have logical access to and process Customer Personal Data in order to comply with their contractual duties.

Term refers to the period from the Terms Effective Date until the end of provision of the services under the Agreement.

Terms Effective Date refers to the actual date when Customers accepts the Data Processing Terms and Conditions.

Customer is an individual or a legal entity (a controller or a processor) that registers an account in eLama Service, provides Customer Personal Data and agrees to the Terms and Conditions, stipulated in this Agreement.

Such terms as ***controller, data subject, personal data, processing, processor*** and ***supervisory authority*** as used in this Agreement have the meanings given in the GDPR.

1.2. Any reference to a legal or regulatory framework, or other legislative enactment is a reference to it with possible amendments over time.

1.3. The duration of this Agreement takes effect o the Term Effective Data is valid until the data Customer Personal Data is effectively deleted by all the parties to this Agreement.

2. Application of these Data Processing Terms and Conditions

2.1. Application of Data Protection Legislation

These Data Processing Terms will only apply to the extent that the Data Protection Legislation applies to the processing of Customer Personal Data, including:

(a) the processing is in the context of the activities of an establishment of the Customer in the EEA or/and Brazil; and/or

(b) Customer Personal Data is personal data relating to data subjects who are in the EEA or Brazil and the processing relates to the offering to them of services or the monitoring of their behavior in the EEA or/and Brazil.

2.2. Application to Data Processing Services

The terms and conditions of this Data Processing Agreement will only apply to the services that the parties agreed to in this Agreement by, for example:

- the Services for which Customer clicked to accept these terms and conditions; and/or
- if the Agreement incorporates these Data Processing Terms and Conditions by reference; and/or
- involves the Processor Services that are the subject of the Agreement.

3. Processing of Personal Data

3.1. Processor and Controller Responsibilities

The parties acknowledge and agree that:

- eLama is a processor or subprocessor of Customer Personal Data under the Data Protection Legislation;
- the Agreement describes the subject and details of the processing of Customer Personal Data (Addendum I);
- the Customer is a controller or processor, as applicable, of Customer Personal Data under the Data Protection Legislation; and
- all parties to this Agreement will comply with their obligations under the Data Protection Legislation with respect to the processing of Customer Personal Data and exercise due diligence to ensure data security and lawful use of Customer Personal Data.

3.2. Authorisation by Third Party Controller

In cases, where the Customer is a data processor, the Customer confirms to the DPS Provider that the instructions given and actions, authorized by the Customer with regards to Customer Personal Data, including its appointment of the DPS Provider as another processor, have been authorized by the relevant controller.

3.3. Customer’s Instructions

By entering into this Agreement, the Customer instructs the DPS Provider to process Customer Personal Data exclusively in accordance with applicable legislation and Terms and Conditions of this Agreement and further documented written instructions acknowledged and agreed upon by the parties to this Agreement for the purpose of Data Processing Agreement. This includes, but is not limited to the provision of the Services by the DPS Provider, technical support, required to comply with the obligations of the parties, the direct and indirect use of the DPS Provider Services.

3.4. The DPS Provider´s Compliance with Instructions

The DPS Provider agrees with and warrants to comply with the instructions, described in Section 3.3., unless the Data Protection law to which the DPS Provider is subject requires other processing of Customer Personal Data by the DPS Provider. In this case, the DPS Provider will inform the Customer immediately (unless the law prohibits the DPS Provider to do so).

3.5. Supplementary Service

If the Customer decides to use a Supplementary Service, the DPS Provider, if and when required can allow the Supplementary Service to access Customer Personal Data to ensure the efficiency and viability of the inter-operational service between the DPS Service and Supplementary Services.

4. Deleting Personal Data

4.1. When Data Deleted During the Agreement Term

During the term of the Agreement, if the functionality of the DPS Provider does not include the option for the Customer to delete (or request the deletion through the system) Customer Personal Data, then DPS Provider will comply with the following:

- any reasonable request from the Customer to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the DPS Services and unless the relevant Data Protection law requires storage for the best public interest;
- such request should be sent by the Customer via the Notification Email Address;
- the request for deletion of Customer Personal Data can be done for Customer Personal Data specifically associated with the Notification Email Address, from which such request is sent.

4.2. When Data is Deleted after the Expiration Date of the Agreement

After the expiration of the Agreement, the Customer should instruct the DPS Provider via the Notification Email Address to delete all Customer Personal Data, associated with such address from the system and (affiliate subprocessor servers and systems) in compliance with the applicable law. The DPS Provider will comply with this instruction within a maximum period of 180 days, unless the relevant Data Protection law requires storage for the best interests of public.

5. Data Security

5.1. The DPS Provider Security Measures and Due Diligence

The DPS Provider assumes the responsibility to implement and maintain technical and organizational measures and structure to protect Customer Personal Data against Data Incidents. Such technical and organizational measures are described in Addendum II (the “Security Measures”).

The DPS Provider can make necessary and implementary update of the Data Security Measures, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

5.2. Security Compliance by employees and contractors of the DPS Provider

The DPS Provider assumes responsibility to exercise due diligence and take the appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent to which it applies to their scope of responsibility and access to Customer Personal Data.

5.3. The DPS Provider Due Diligence

The Customer agrees that the DPS Provider will (to the extent to which Customer Personal Data is available and accessible to the DPS Provider) exercise due diligence in ensuring compliance and assisting the Customer where appropriate, with any obligations of the Customer in respect of security of Customer Personal Data and avoidance of Data Incidents, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by complying with all the sections of this Agreement.

5.4. Data Incidents

5.4.1. Incident Notification

If and when the DPS Provider becomes aware of a Data Incident, the DPS Provider assumes the responsibility to:

- notify the Customer of the Data Incident immediately (or as soon as it is possible) and without undue delay;
- take reasonable steps to minimize the potential and actual damage and secure Customer Personal Data.

5.4.2. Details of Data Incident

Incident notifications will outline and detail the Data Incident and the overview of the measures that are undertaken by the DPS Provider to minimize it along with the extent to which the Data Incident may affect the Customer, based on reasonable assumption of the DPS Provider.

5.4.3. Delivery of Incident Notification

The DPS Provider assumes the responsibility to inform the Customer about the Data Incident through the Notification Email Address or, at the DPS Provider´s discretion (including, but not limited to the situations where the Customer has not provided a valid Notification Email Address), by other direct communication method (such as phone call or an in-person meeting). The Customer is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

5.4.4. Third Party Notifications

The Customer is solely responsible for complying with the regulations and laws of Incident Notification applicable to the Customer and required to fulfill demand and regulations of a Third Party provider.

5.4.5. The Essence of Incident Notification

The provision and delivery of Incident notification has only informative nature and cannot be considered and used as the acknowledgement by the DPS Provider of any fault or liability with regards to the Data Incident.

5.5. Customer's Security Measures Responsibilities and Due Diligence

5.5.1. Customer's Security Measures Responsibilities

By accepting this Agreement the Customer guarantees that, without prejudice to the DPS Provider´s obligations under Sections 5.1 to Section 5.4, the Customer is solely responsible for the use of the DPS Provider´s Services, including:

- exercise due diligence to ensure the level of security appropriate to the risk with regards to Customer Personal Data; and
- the Customer acknowledges that the DPS Provider has no obligation to protect Customer Personal Data that the Customer elects to store or transfer outside of the DPS Provider´s and its Subprocessors' systems.

5.6. Reviews and Audits of Compliance

5.6.1. Customer´s Security Documentation and Audit Rights

The DPS Provider will make the Security Documentation available for review by the Customer, upon request sent via Notification Email Address. This being said, the term for answering to such a request shall be no longer than 60 (sixty) calendar days from the date of the request receipt. Additionally, the Customer or a third party auditor appointed by the Customer has a right to conduct audits (including inspections) to verify the DPS Provider´s compliance with its obligations under this Agreement.

5.6.2. Additional Business Terms for Audits.

- The Customer will send any request for an audit under to the DPS Provider as described in the section described in Section 6 of this Agreement.
- When the request is received by the DPS Provider, the parties will agree on the start date, time and period of such audit, as well as the scope and security and confidentiality controls and measures that should be applied for the audit.
- The DPS Provider may object and reject a third party auditor, appointed by the Customer if the DPS Provider or its subcontractors, subprocessors and other affiliate and third party contractors decide that the appointed auditor is not qualified enough to conduct such audit. In such case the Customer will appoint another auditor.
- The DPS Provider may charge a reasonable fee for such audit. In case of such applicable fees, the Customer will be informed and will approve the fees.

Under no circumstances the auditor can request the DPS provider to disclose the following information:

- any data of any other customer of the DPS Provider and its affiliates;
- any DPS Provider's and its affiliates´ and third parties´ internal accounting or financial information;
- any trade secret of the DPS Provider and its affiliates;

- any information that in the DPS Provider´s opinion could compromise Customer Personal Data, the DPS Provider´s and its affiliate and third party provider´s systems, services, premises (or other facilities and property);
- information that may result in breach of DPS Agreements with other Customers.

6. Contacting DPS Provider and Processing Records

6.1. Contacting the DPS Provider

The Customer may contact the DPS Provider in relation to the exercise of its rights under this Agreement via Notification Email Address or phone. Official requests for audit or other inspections, Data Deletion or similar should always be sent in written via the Notification Email Address.

6.2. The DPS Provider´s Processing Records.

By entering into this Agreement the Customer acknowledges that the DPS Provider is required under the GDPR to:

- collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which the DPS Provider is acting and (if applicable) of such processor's or controller's local representative and data protection officer;
- make such information available to the supervisory authorities on request, including the cases where such information has to be provided by the Customer to the DPS Provider upon request from the supervisory authorities under applicable laws. The Customer, therefore, assumes the responsibility to keep the contact information accurate and up-to-date.

7. Impact Assessments and Consultations

By accepting this Agreement the Customer acknowledges and agrees that the DPS Provider will (within its scope and access to the information) assist the Customer in ensuring compliance with any obligations that the Customer may have for data protection, impact assessments and prior consultation, including (if applicable) the Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

- providing the Security Documentation in accordance with Section 5;
- providing the information contained in this Agreement;
- providing other information on Data Processing and processing of Customer Personal Data, relevant and applicable to the situation, unless the same is prohibited by applicable legislation.

8. Data Subject Rights

8.1. Responses to Data Subject Requests

If the DPS Provider receives a request from a Data Subject in relation to Customer Personal Data, the DPS Provider will:

- if the Data Subject makes the contact information available to the DPS Provider and allows direct contact from the DPS Provider, the DPS Provider will respond directly to the Data Subject's request.
- if the Data Subject submits the request to the Customer, the Customer will be responsible for responding to such request.

8.2. The DPS Provider's Assistance to Data Subject Requests

The Customer agrees that the DPS Provider will (taking into account Customer Processing Data clauses of Article 11 of the GDPR) assist the Customer in fulfilling any obligation of the Customer to respond to requests by data subjects. Such assistance includes the requests received by the Customer with regards to exercising the Data Subject's rights laid down in Chapter III of the GDPR, by:

- providing the functionality of the DPS Provider Services;
- complying with the commitments, outlined in Section 8.1;
- if applicable to the DPS Provider´s services, explaining and guiding the Customer through the explicit details on what information is being stored by eLama and partners.

9. Data Transfers

9.1 Data Storage and Processing Facilities

The Customer agrees that the DPS Provider may, subject to Section 9.2., store and process Customer Personal Data internationally to the countries in which the DPS Provider or any of its affiliate or third party Subprocessors maintains facilities

9.2 International Data Transfers

The DPS Provider shall in advance of any such transfer, ensure that a legal mechanism to achieve adequacy with respect to that processing is in place. This being said, the Customer hereby agrees with the list of Subprocessors of the DPS Provider, indicated in clause 10.2 of this Agreement.

10. Subprocessors

10.1 Consent to Subprocessor Engagement.

By accepting the terms and conditions of this Agreement, the Customer specifically authorizes the engagement of the DPS Provider´s Affiliates as Subprocessors ("DPS Provider´s Affiliate Subprocessors"). In addition, the Customer generally authorises the engagement of any other third parties as Subprocessors ("Third Party Subprocessors").

10.2 Information about Subprocessors

Information about Subprocessors is available at https://elama.global/contacts/. This information is agreed by the parties hereto to be a part of this Agreement.

10.3 Requirements for Subprocessor Engagement

When working and engaging any Subprocessor, the DPS Provider will sign a written contract with such party that ensures and communicates that:

- the engaged Subprocessor only accesses and uses Customer Personal Data applicable to the scope and required to perform the obligations that the DPS Provider delegates to it, and does so in compliance with the applicable laws, the eLama Global Data Processing Terms and Conditions and any other relevant regulations and legislation;
- if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Subprocessor; and the Subprocessor remains fully liable for all the obligations that are delegated to him by the DPS Provider.

10.4. Object to Subprocessor Changes

If a new Third Party Subprocessor is to be engaged and work with the DPS Provider during the term of the Agreement, the DPS Provider assumes the responsibility to, at least 15 days before the new Third Party Subprocessor processes any Customer Personal Data, inform the Customer of such change and provide the name and location of the Third Party Subprocessor. Such information will be sent to the Notification Email Address of the Customer.

The Customer has a right to object to any new Third Party Subprocessor, in which case the current Agreement will be terminated immediately, on condition that the Customer provides such notice within 90 days of being informed of the engagement of the new Third Party Subprocessor as described in Section 10.4 in written form as outlined in Section 6. Such termination notice can only be done by the Customer or the party specifically authorized by the Customer and known to the DPS Provider.

11. Liability

If the Agreement is governed by the laws of:

- a state of the EEU or Brazil, then, notwithstanding anything else in the Agreement, the total individual and mutual liability of the parties to this Agreement will be limited to the maximum monetary or payment-based amount and clauses of the relevant Data Protection Legislation;
- countries other than Brazil or EEU member states, the total individual and mutual liability of the parties to this Agreement will be subject to the clauses of this Agreement and the relevant Data Protection Legislation of the respective states.

12. Effect of these Data Processing Terms

If there is any conflict or inconsistency between the terms of this Agreement and the remainder of the Agreements with the Customer, the terms of this eLama Global Data Processing Terms and Conditions will govern. Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.

13. Changes to this Agreement

13.1 Changes to URLs

In the eventuality the DPS Provider requires to change the references and URLs, mentioned in this Agreement, the Customer may access these links in this Agreement as updated. The DPS Provider may only change the content and the data under the URLs, outlining the list of the contractors and processors with the intention to:

- to reflect a change to the name of the service provided;
- to remove a service where either the contract for this service is terminated or the Customer gave the consent to do so.
- to add a new service.

13.2 Changes to Data Processing Terms and Conditions

The DPS Provider can change the Terms and Conditions of this Agreement if:

- the conditions of Section 13.1 of this Agreement apply;
- the DPS Provider changes the name or legal details;
- the change is required to comply with any of the applicable laws and regulations, or on demand of the authorities under the court order.

The DPS Provider will ensure that the following conditions are met to implement the change:

- the change does not reduce, in reasonable opinion of the DPS Provider the Data Security, outlined in this Agreement;
- the change does not change the scope or remove the approved restrictions in this Agreement;
- the change does not undermine the DPS Provider commitment to comply with the instructions as outlined in Section 3;
- the change will not result in a negative material impact on the Customer's rights under this Agreement as reasonably determined by the DPS Provider.

13.3. Communication of Changes to the Customer

If any change is done to the Agreement, the DPS Provider will duly inform the Customer at least 30 days (unless otherwise required by the applicable law or regulation) before the change will become effective. This communication will be done via Notification Email Address and (or) the Customer interface in the DPS Provider's system. If the Customer objects the change, it may terminate the Agreement by giving a written notice from the Notification Email Address. Such notice can only be given by the Customer itself or by a specifically authorized party, known to the DPS Provider.

Addendum I: Subject and Details of the Data Processing

Nature and Purpose of the Processing

The DPS Provider will process data in accordance with Section 3 of this Agreement. Processing includes the collecting, recording, organizing, structuring, storing, altering, retrieving, using, combining, erasing and destroying of Customer Personal Data with the purpose of providing the Services and any support and assistance, related to these Services to the Customer in accordance with this Agreement.

Subject Matter

The subject matter of processing of Personal Data by the DPS Provider is the provision of the Services to the Customer that involves the processing of Customer Personal Data. Customer Personal Data will be subject to those processing activities as may be specified the Customer's instructions.

Duration of the Processing

The Term plus the period from expiry of the Term until deletion of all Customer Personal Data by the DPS Provider in accordance with this Agreement.

Types of Personal Data

The DPS Provider processes the following types of personal data: contact information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as email data and other electronic data submitted, stored, sent, or received by the Customer.

Categories of Data Subjects

Data subjects about whom personal data is transferred to the DPS Provider in relation to the Services by, by order or on behalf of the Customer.

Addendum 2: Security Measures (Technical and Organization Measures in respect to Data Collection, Processing and Storage)

The DPS Provider has implemented and will maintain the technical and organizational security measures reasonably required for safeguarding data against corruption, loss or access from any unauthorized third party.

The DPS Provider uses geographically distributed data centers provided by Amazon Web Services (AWS). For information about the controls implemented by AWS towards their data centers, please refer to https://aws.amazon.com/compliance/data-center/controls/. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. The DPS Provider transfers data via Internet standard protocols.

Details of Technical and Organizational Measures currently maintained by the DPS Provider are listed below:

General description of measures	Description of measures implemented
Access control Preventing unauthorized persons from gaining access to premises, systems and data	• Premises access control system • System and data access limited to authorized personnel (based on roles and need to know) • Database security controls restrict access • Protocol of logons • Anti-virus and firewall systems • Signed confidentiality undertakings • Surveillance systems (alarm system, door prop alarm, 24x7 CCTV)
Transmission control Ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to review and establish which bodies are to receive the personal data	• Encrypted transfer (Secure Socket Layer/Transport Layer Security (SSL/TLS) in connection with valid certificates, secure shell, Secure Network Communication, Secure FTP (SFTP), IPSec, VPN technologies • Logging
Input control Ensuring that it is possible to review and establish whether and by whom personal data have been input into data processing systems, modified or removed	• Access rights based on roles and need to know • Approval process for access rights; periodical reviews and audits • Logging

The DPS Provider reserves the right to make changes and updates to the above list of applied Technical and Organizational Measures to accommodate developments in the industry from time to time. The latest current details of Technical and Organizational Measures maintained by the DPS Provider can always be accessed at https://elama.global/contacts/.

1 November 2018