Exhibit A

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is an integral part of the agreement executed between the parties ("**Agreement**"), for the purpose of using the Services, as defined under the Agreement. Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

This DPA sets forth the parties' responsibilities and obligations regarding the Processing of Personal Data (as such terms are defined below) during the course of the engagement between the parties.

1. **Definitions**

1.1. **"Adequate Country"** is a country that an adequacy decision from the European Commission.

1.2. "**Affiliates**" means any entity which is controlled by, controls or is in common control with one of the parties.

1.3. "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018, as may be amended as well as all regulations promulgated thereunder from time to time.

1.4. The terms "**Controller**," "**Processor**," "**Data Subject**," "**Processing**," (and "**Process**") "**Personal Data Breach**," and "**Special Categories of Personal Data**" shall all have the same meanings as ascribed to them in the EU Data Protection Law and the LGDP. The terms "**Business**," "**Business Purpose**," "**Consumer**," "**Service Provider**," "Sale," and "**Sell**" shall have the same meaning as ascribed to them in the CCPA. "**Data Subject**" shall also mean and refer to a "**Consumer**," as such term is defined in the CCPA.

1.5. "**Data Protection Law**" means any and all applicable privacy and data protection laws and regulations (including, where applicable, the EU Data Protection Law, the LGPD and the CCPA) as may be amended or superseded from time to time.

1.6. "**EU Data Protection Law**" means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"); (ii) Regulation 2018/1725; (iii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (iv) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); (v) any legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

1.7. "**LGPD**" means the Brazilian General Data Protection Law (as amended by Law No. 13,853/2019), as may be amended from time to time.

1.8. "**Personal Data**" or "**Personal Information**" means any information which can be related, describes, or is capable of being associated with, an identifiable individual, including any information that can be linked to an individual or used to directly or indirectly identify an individual or Data Subject.

1.9. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data Breach will be considered a Security Incident.

1.10. "**Standard Contractual Clauses**" mean the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found here: Standard Contractual Clauses.

1.11. "**UK GDPR**" means th7e Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

1.12. "**UK SCC**" means where the UK GDPR applies, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR for transferring Personal Data outside of the EEA or UK.

2. **Parties' Roles**

2.1. The parties agree and acknowledge that the Company is acting as a Processor and you are acting as a Controller with respect to the Processing of Controller's Personal Data. The purpose, subject matter and duration of the Processing carried out by the Processor on behalf of the Controller, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **ANNEX I** attached hereto ("**Controller Data**").

2.2. For the purpose of the CCPA (and to the extent applicable), Controller is the Business and the Company is the Service Provider. Each party shall be individually and separately responsible for complying with the obligations that apply to such party under applicable Data Protection Law.

2.3. The Controller acknowledge and agrees that the Company may process and utilize the Controller Data in order to enrich and improve its Services and shall use the Controller Data to provide insights and Marketing and Optimization Tools.

3. **Representations and Warranties**

3.1. The Controller represents and warrants that: (i) its Processing instructions shall comply with applicable Data Protection Law; (ii) it will comply with Data Protection Law, specifically with regards to the lawful basis principal for Processing Personal Data; and (iii) it obtained the needed consents to ensure the Processing of the Controller Data by Processor is lawful and that all needed disclosures subject to Article 12-14 of the GDPR were displayed.

3.2. The Company represents and warrants that: (i) it shall process Personal Data, as set forth under Article 28(3) of the GDPR, on behalf of the Controller, solely for the purpose of providing the Services, and for the pursuit of a Business Purpose as set forth under the CCPA, all in accordance with Controller's written instructions including the Agreement and this DPA;

(ii) in the event the Company is required under applicable laws, including the Data Protection Law or any union or member state regulation, to Process Personal Data other than as instructed by Controller, the Company shall inform the Controller of such requirement prior to Processing such Personal Data, unless prohibited under applicable law; and (iii) it will provide reasonable cooperation and assistance to Controller in ensuring compliance with its obligation to carry out data protection impact assessments with respect to the processing of Personal Data and with its obligation to consult with the supervisory authority (as applicable).

4. **Processing of Personal Data and Compliance with Data Protection Law**

4.1. The Controller represents and warrants that Special Categories of Personal Data or Sensitive Data shall not be Processed or shared in connection with the performance of the Services, unless the Company agrees in writing for such data to be shared with it. Unless otherwise agreed to in writing by the parties, the Controller shall not share any Personal Data with the Company that contains Personal Data relating to children under the age of 16. Notwithstanding the above, in the event Special Categories of Personal Data or Sensitive Data the Company shall implement specific restrictions and safeguards in order to protect such Special Categories of Personal Data.

5. **Company Personnel**

5.1. The Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Personal Data. The Company shall ensure that the individuals who are authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and ensure that such personnel are aware of their responsibilities under this DPA and any applicable Data Protection Law.

6. **Rights of Data Subjects and Parties Cooperation Obligations**

6.1. It is agreed that where the Company receives a request from a Data Subject or an applicable authority in respect to Personal Data Processed by the Company, where relevant, the Company will direct the Data Subject or the applicable authority to the Controller in order to enable the Controller to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable law. The Company shall provide the Controller with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's or applicable authority's request, to the extent permitted under Data Protection Law.

6.2. Where applicable, the Company shall assist the Controller to ensure that Personal Data Processed is accurate and up to date, by informing the Controller without delay if the Company becomes aware that the Personal Data that it is processing is inaccurate or has become outdated.

7. **Do Not Sale of Personal Information**

7.1. It is the Controller's sole responsibility and liability to determine whether the sharing or transferring of Personal Information of Consumers during the course of the Services constitutes a Sale of Personal Information and it is also the Controller's responsibility to comply with the applicable CCPA requirements in this regard, including providing a "**Do Not Sell**" signal for end users who have exercised their right to opt out, where applicable.

8. **Sub-Processor**

8.1. The Controller acknowledges that the Company may transfer Personal Data to and otherwise interact with third party data processors ("**Sub-Processor**"). The Controller hereby authorizes the Company to engage and appoint Sub-Processors to Process Personal Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. The Company may continue to use those Sub-Processors which are already engaged by it, as listed in **ANNEX III**, and may engage an additional or replace an existing Sub-Processor to process Personal Data. The Company shall provide Controller with 30 days prior written notice of its intention to replace or add a Sub-Processor. In case the Controller has not objected to the adding or replacement of a Sub-Processor, such Sub-Processor shall be considered as approved by the Controller upon the end of such 30 day period. The sole remedy of the Controller in the event that it has objected to the replacement or addition of any particular Sub-Processor will be to terminate the Agreement.

8.2. The Company shall, where it engages any Sub-Processor, impose, through a legally binding contract between itself and the Sub-Processor, data protection obligations as required under applicable Data Protection Law. The Company shall ensure that such contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Law. The Company shall, upon written request by the Controller, provide the Controller with such Sub-Processor's agreement and any subsequent amendments thereto. The Company may redact certain sections or text of the agreement with any particular Sub-Processor prior to sharing the copy of such agreement with the Controller, if the Company, at its sole discretion, determined that it is necessary to do so in order to protect trade secrets or any other confidential information (including Personal Data).

8.3. The Processor shall remain fully responsible to the Controller for the performance of the Sub-Processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-Processor to fulfil its contractual obligations.

9. **Technical and Organizational Measures**

9.1. 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, without prejudice to any other security standards agreed upon by the parties, the Company shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Processing

and which will be in accordance with best industry practices for the protection data from a Security Incident. The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

9.2. Technical and organizational measures implemented by Ongage (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons are ISO 27001 certified. Upon Customer request Ongage shall provide with Ongage's ISO certification.

9.3. The security measures are further detailed in **ANNEX II**.

10. **Security Incident**

10.1. The Company will notify the Controller upon becoming aware of any confirmed Security Incident involving the Personal Data in Company's possession or control. The Company will: (i) take such steps as are necessary to contain, remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate with the Controller and provide the Controller with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; (iii) notify the Controller in writing of any request, inspection, audit or investigation by a supervisory authority or other authority; (iv) keep the Controller informed of all material developments in connection with the Security Incident and execute a response plan to address the Security Incident; and (v) co-operate with the Controller and assist Controller with the Controller's obligation to notify affected individuals in the case of a Security Incident.

10.2. Company's notification regarding or in response to a Security Incident under this Section 9 shall not be construed as an acknowledgment by the Company of any fault or liability with respect to the Security Incident.

11. **Audit Rights**

11.1. The Company shall respond promptly and adequately with respect to inquiries from the Controller about the Processing of Personal Data in accordance with this DPA. Company shall make available to the Controller all information necessary to demonstrate compliance with the obligations under the EU Data Protection Law.

11.2. The Company shall make available, solely upon prior written notice and no more than once per year, except for upon the occurrence of a Security Incident, to a reputable auditor nominated by the Controller, information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Personal Data ("**Audit**") in accordance with the terms and conditions hereunder. The auditor shall be subject to the terms of this DPA and standard confidentiality obligations (including towards third parties). The Company may object to an auditor appointed by the Controller in the event the Company reasonably

believes the auditor is not suitably qualified or independent, is a competitor of the Company or is otherwise unsuitable ("**Objection Notice**"). The Controller will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from the Company. Controller shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, avoid causing any damage, injury or disruption to the Company's premises, equipment, personnel and business during the Audit. Any and all conclusions of such Audit shall be confidential and reported back to the Company immediately.

12. **Data Transfer**

12.1. You acknowledge and agrees that in order to provide the Services Ongage might transfer (or access) Controller Data from countries outside the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**") as detailed herein.

12.2. The parties acknowledge that EU Data Protection Law does not require Standard Contractual Clauses or an alternative transfer solution in order for Controller Data to be processed in or transferred to an Adequate Country ("**Permitted Transfers**").

12.3. In the event the Processing includes transferring of Personal Data from the EEA, Switzerland or the UK to other countries and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Ongage for the lawful transfer of processing Personal Data outside the EEA, Switzerland or the UK, as applicable or is not exempt under Article 49 of the GDPR (collectively "**Restricted Transfer**"), the following shall apply:

12.3.1. In order to maintain the integrity, security and confidentiality of the Personal Data, a Restricted Transfer shall be subject, in addition to the terms of this DPA, to the terms and obligations of the **Module II** of the Standard Contractual Clauses in which Ongage shall be deemed as the Data Importer and the Controller shall be deemed as the Data Exporter.

12.3.2. The purpose and description of the transfer shall be detailed in **ANNEX I**.

12.3.3. The UK SCC shall incorporate **ANNEX I, II and III** herein.

12.4. You further agrees that where Ongage engages a Sub-Processor, and those processing activities include a Restricted Transfer, Ongage and the Sub-Processor shall be bound by the Standard Contractual Clauses in which Ongage shall be deemed as the Data Exporter and the Sub-Processor shall be deemed as the Data Importer. For the purposes of such engagement, Ongage r and the Sub-Processor will enter into **Module III** of the Standard Contractual Clauses.

12.5. Subject to Clause 13 of Standard Contractual Clauses, Ongage agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Standard Contractual Clauses. Notwithstanding the above the UK SCCs shall be governed by the laws of England and Wales.

12.6. Measures and assurances regarding U.S. government surveillance ("**Additional Safeguards**") are further detailed in **ANNEX II**.

13. **Termination**

13.1. This DPA shall be effective as of the effective date of the Agreement and shall automatically be terminated upon the termination of the Agreement. The Controller shall be entitled to suspend the Processing of Controller Data in the event the Company is in breach of Data Protection Laws, this DPA or a binding decision of a competent court or the competent supervisory authority

13.2. The Company shall be entitled to terminate this DPA or terminate the Processing of Controller Data in the event the Processing of Personal Data under the Controller's instructions or this DPA infringe applicable legal requirements. Such termination shall be subject to informing the Controller and the Customer insists on compliance with the instructions.

13.3. Following the termination of this DPA, the Company shall, at the Controller's discretion: (i) delete all of the Controller's Personal Data processed on behalf of the Controller and certify to the Controller that it has done so; or (ii) return all of the Controller's Personal Data to the Controller and delete any existing copies stored by the Company. Company shall be permitted to retain or store any of Controller's Personal Data that it is required to retain or store under applicable law or in accordance with any regulatory requirements. Company shall continue to comply with this DPA until the Controller's Personal Data has been deleted or returned, in accordance with the above.

14. **Conflict**

14.1. In the event of a conflict between the terms and conditions of this DPA and the Agreement or IO, this DPA shall prevail.

ANNEX I

DETAILS OF PROCESSING AND TRANSFERRING OF CONTROLLER PERSONAL DATA

This Annex I include certain details of the Processing of Personal Data as required by Article 28(3) GDPR and details of transferring Personal Data subject to the Standard Contractual Clauses.

Categories of data subjects whose personal data is processed or transferred:

- Controller's employees (i.e., Authorized Users)
- Controller's Recipients

Categories of personal data processed and transferred:

- Recipients:
  - full Name
  - email address
  - phone number
  - job title
  - geographical location (including home and/or company address)
  - Recipient's behavior segments: email action (click, open) time of clicking and opening email, email bounce date and email categorize, profiling preference and behavior.

Sensitive data processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measure:

NA

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing and transferring:

Processing, hosting and transmission.

Purpose(s) for which the personal data is processed or transferred on behalf of the controller:

Providing the Services

Duration of the processing:

For the duration of the Services according to the main agreement.

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing.
The sub-processors are hosting services, storage providers, all of the above is applicable to the sub-processors.

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

The security objectives of the Company are identified and managed to maintain a high level of security and consists of the following (concerning all data assets and systems):

- **Availability** - information and associated assets should be accessible to authorized users when required. The computer network must be resilient. The Company must detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information.
- **Confidentiality** - ensuring that information is only accessible to those authorized to access it, on a need-to-know-basis.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of electronic data.

Physical Access Control

The Company ensures the protection of the data servers which store the Personal Data for the Company from unwanted physical access.

The Personal Data that is processed by the Company and which the Company is the Controller of (as such term is defined under the GDPR) is stored on Amazon Web Services.

The data processed by the Company as a Processor (as such term is defined under the GDPR) may be stored on Amazon Web Services (AWS). Please see AWS's security measures here. The Company also secures physical access to its offices by ensuring that only authorized individuals such as employees and authorized external parties (maintenance staff, visitors, etc.) can access the Company's offices by using security locks and an alarm system, amongst other measures as well.

System Control

Access to the Company's database is highly restricted in order to ensure that only the relevant personnel who have received prior approval can access the database. The Company has also implemented appropriate safeguards related to remote access and wireless computing capabilities. Employees are assigned private passwords that allow strict access or use to Personal Data, all in accordance with such employee's position, and solely to the extent such access or use is required. There is constant monitoring of access to the Personal Data and the passwords used to gain access. The Company is using automated tools to identify non-human login attempts and rate-limiting login attempts to minimize the risk of a brute force attack.

Data Access Control

User authentication measures have been put in place in order to ensure that access to Personal Data is restricted solely to those employees who have been given permission to access it and to ensure that the Personal Data is not accessed, modified, copied, used, transferred or deleted without specific authorization for such actions to be done. Any access to Personal Data, as well as any action performed involving the use of Personal Data requires a password and user name, which is routinely changed, as well as blocked when applicable. Each employee is able to perform actions solely in accordance with the permissions granted to him by the Company. Furthermore, the Company conducts ongoing reviews of the employees who have been given authorization to access Personal Data, in order to

assess whether such access is still required. The Company revokes access to Personal Data immediately upon termination of employment. Authorized individuals can only access Personal Data that are located in their individual profiles.

Organizational and Operational Security

The Company puts a lot of effort and invests a lot of resources into ensuring that the Company's security policies and practices are being complied with, including by continuously providing employees with training with respect to such security policies and practices. The Company strives to raise awareness regarding the risks involved in the processing of Personal Data. In addition, the Company has implemented applicable safeguards for its hardware and software, including by installing firewalls and anti-virus software on applicable Company hardware and software, in order to protect against malicious software.

Transfer Control

All transfers of Personal Data between the client, the Company's service providers and the Company's servers are protected by the use of encryption safeguards, including the encryption of the Personal Data prior to the transfer of any Personal Data. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

Input Control

The Company ensures the transparency of input controls, including changing and the deletion of data.

Availability Control

The Company maintains backup policies and associated measures. Such backup policies include permanent monitoring of operational parameters as relevant to the backup operations. Furthermore, the Company's servers include an automated backup procedure. The Company also conducts regular controls of the condition and labelling of data storage devices for data security. The Company ensures that regular checks are carried out to determine whether it is possible to undo the backup, as required and applicable.

Data Retention

Personal Data is retained for as long as needed for us to provide our services or as required under applicable laws.

Job Control and Third Party Contractors and Service Providers

All of the Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable provisions binding them to comply with applicable data security practices. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company implements certain repercussions in order to ensure compliance with the Company's policies. In addition, prior to the Company's engagement with third party contractors, the Company undertakes diligence reviews of such third party contractors. The Company agrees with third party contractors on effective rights of control with respect to any Personal Data processed on behalf of the Company. The Company ensures that it enters into data protection agreements with all of its clients and service providers.

Compliance Programs

Ongage operations, policies and procedures are audited regularly to ensure Ongage meets all standards expected as a cloud system provider. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. Ongage's systems and services were audited and verified by ISO 27001.

Ongage's customers remain responsible for complying with applicable compliance laws, regulations and privacy programs in addition to Ongage's compliance with privacy and security regulations.

Penetration Testing

External penetration test is performed on an annual basis. The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. The penetration tests and security scans are performed by a reputable Third-party vendor. In addition, The Company conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment. Actions are taken to remediate identified deficiencies on a timely basis. Vulnerability scans is performed using external tools, in order to detect potential security breaches

Additional Safeguard

Measures and assurances regarding U.S. government surveillance ("**Additional Safeguards**") have been implemented due to the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems decision ("**Schrems II**"), these measures include the following:

- encryption both in transit and at rest;
- As of the date of this DPA, Ongage has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II decision.
- No court has found Ongage to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.
- Ongage shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).
- Ongage shall use all available legal mechanisms to challenge any demands for data access through national security process that Ongage receives, as well as any non-disclosure provisions attached thereto.
- Ongage will notify Customer if Ongage can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

ANNEX III

List of Sub-Processors

Ongage's approved Sub-Processors list, as may be amended from time to time according to the terms of this DPA:

- Amazon Web Services (AWS)