ALL IN ONE EMAIL, LLC
DATA PROCESSING TERMS AND CONDITIONS

These ALL IN ONE EMAIL, LLC Data Processing Terms and Conditions (referred to hereafter as the "**DPA**") are incorporated by reference into and are integrated with the Email Services Agreement ("**Agreement**") between Company and Customer for purposes of using the Services, as defined under the Agreement. All capitalized terms herein which are not otherwise defined, shall have the definition set forth in Agreement and the Company's Standard Terms and Conditions, located at https://www.allinoneemail.com/terms-of-services.pdf (the "Terms").

In recognition that the Services may require Processing by the Company of Personal Data, as defined below, on the Customer's behalf subject to the terms and conditions of this DPA; and based on the desire to comply United States, California and other data protection laws, Company and Customer agree that Processing of any Personal Data shall, in addition to the standard Terms, be further subject to the terms and conditions set forth herein.

1. APPLICATION OF THE DPA

1.1. This DPA reflect the Parties' agreement on the processing of Personal Data in connection with the Services and the Agreement and in accordance with Data Protection Law. This DPA will only apply to the extent: **(i)** Company Processes Personal Data that is made available, directly or indirectly, by Customer (or on its behalf) in connection with the Services and the Agreement; and **(ii)** Data Protection Law apply to the Processing of Personal Data.

1.2. The terms and conditions of this DPA shall govern and control to the extent of any conflict with any other terms and conditions of the ESA.

2. DEFINITIONS

2.1. "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018, as amended by the 2020 California Privacy Rights Act, and all regulations promulgated thereunder from time to time.

2.2. "**Customer Data**" means any and all Personal Data provided by the Customer to Company in performance of the ESA, as further described in **Annex I** attached herein.

2.3. The terms "**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Processing**" (and "**Process**"), "**Personal Data Breach**", "**Special Categories of Personal Data**" and "**Supervisory Authority**", shall all have the same meanings as ascribed to them in the EU Data Protection Law. The terms "**Business Purpose**", "**Consumer**", "**Cross Context Behavioral Advertising**", **"First-Party Business",** "**Service Provider**", "**Share**", "**Sale**", "**Third-Party Business**" and "**Sell"** shall have the same meaning as ascribed to them in the CCPA. "**Data Subject**" shall also mean and refer to "**Consumer**", as such term defined in the CCPA, "**Personal Data**" shall include "**Personal Information**" under this DPA.

2.4. "**Data Protection Law**" means applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, the CCPA, and other U.S. state data protection laws) as may be

amended or superseded from time to time.

2.5. "**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.

2.6. "**Security Incident**" means any significant accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data (including Customer Data).

2.7. "**UK Data Protection Laws**" shall mean the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law as the UK GDPR, as amended, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time.

2.8. "**UK GDPR**" shall mean the GDPR as it forms part of domestic law in the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time). Any references to the GDPR in this DPA shall mean the GDPR or UK GDPR depending on the applicable Law.

3. ROLES AND DETAILS OF PROCESSING

3.1. The Parties agree and acknowledge that under the performance of their obligations set forth in the Agreement, and with respect to the Processing of Customer Data, Company is acting as a Data Processor and Customer is acting as a Data Controller. Each Party shall be individually and separately responsible for complying with the obligations that apply to such party under applicable Data Protection Law.

3.2. The 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.

3.3. 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.

3.4. CCPA specifications are further detailed in **Annex IV**.

4. PROCESSING OF PERSONAL DATA

4.1. The Customer represents and warrants that: (i) its Processing instructions shall comply with applicable Data Protection Law, and the Customer acknowledges that, taking into account the nature of the Processing, Company is not in a position to determine whether the Customer's instructions infringe applicable Data Protection Law; and (ii) as between the parties, the Customer undertakes, accepts

and agrees that the Data Subjects do not have a direct relationship with Company and that Company relies on Customer's lawful basis (as required under Data Protection Law). In the event consent is needed under Data Protection Law, the Customer shall ensure that it obtains a proper act of consent from Data Subjects and present all necessary and appropriate notices in accordance with applicable Data Protection Law and other relevant privacy requirements in order to Process Customer Data and enable the lawful transfer and Processing of Customer Data to and by Company, as well as where applicable, provide the Data Subjects with the ability to opt out.

4.2. The Customer represents and warrants that Special Categories of data shall not be Processed or shared in connection with the performance of the Services, unless agreed in writing by Company.

4.3. Company represents and warrants that it shall Process Customer Data, solely for the purpose of providing the Services, all in accordance with Customer's written instructions including the Agreement and this DPA. Notwithstanding the above, in the event Company is required under applicable laws, including Data Protection Law, to Process Customer Data other than as instructed by Customer, Company shall make commercially reasonable efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.

4.4. Each Party shall provide reasonable cooperation with the other Party's undertaking of any data protection impact assessments with respect to the Processing of Customer Data.

4.5. Where applicable, Company shall assist the Customer in ensuring that Personal Data Processed is accurate and up to date, by promptly notifying Customer upon becoming aware that Personal Data it is Processing is inaccurate or has become outdated.

4.6. Company shall take reasonable steps to ensure: (i) 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 Customer Data; (ii) that persons authorized to process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and (iii) that such personnel are aware of their responsibilities under this DPA and any applicable Data Protection Law.

5. DATA SUBJECTS REQUESTS

5.1. Where Company receives a request from a Data Subject or an applicable authority pertaining to Customer Data Processed by Company, Company will direct the Data Subject or the applicable authority to the Customer in order to enable the Customer to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws. Parties shall provide each other 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 the Data Protection Law.

6. SUB-PROCESSING

6.1. The Customer acknowledges that Company may transfer Customer Data to and

otherwise interact with third party data processors ("**Sub-Processor**"). The Customer hereby authorizes Company to engage and appoint such Sub-Processors to Process Customer Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. Company may continue to use those Sub-Processors already engaged by Company, as listed in **Annex III**, or to engage an additional or replace an existing Sub-Processor to process Customer Data, subject to the provision of a thirty (30) day prior notice of its intention to do so to the Customer. In case the Customer has not objected to the adding or replacing of a Sub-Processor within thirty (30) days of Company's notice, such Sub-Processor shall be considered approved by the Customer. In the event the Customer objects to the adding or replacing of a Sub-Processor, Company may, at Company's sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise terminate the Agreement.

6.2. Company shall, where it engages any Sub-Processor, impose, through a legally binding contract between Company and the Sub-Processor, data protection obligations similar to those set out in this DPA. 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.

6.3. Company shall remain responsible to the Customer for the performance of the Sub-Processor's obligations in accordance with this DPA. Company shall notify the Customer of any failure by the Sub-Processor to fulfill its contractual obligations.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

7.1. 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, and without prejudice to any other security standards agreed upon by the parties, Company confirms that it has implemented and will maintain appropriate physical, technical and organizational measures to protect the Customer Data as required under Data Protection Law to ensure lawful processing of Customer Data and safeguard Customer Data from unauthorized, unlawful or accidental processing, access, disclosure, loss, alteration or destruction. The Parties acknowledge that security requirements are constantly changing and that effective security requires the periodic evaluation and improvement of outdated security measures.

7.2. Technical and organizational measures implemented by Company (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 consultation with expert privacy counsel to ensure compliance with Data Protection Law. Upon request, Company shall tender additional information to Customer about the privacy counsel relied upon by Company.

7.3. The security measures are further detailed in **Annex II**.

8. PERSONAL DATA SECURITY INCIDENT

8.1. Company will notify the Customer upon becoming aware of any confirmed Security Incident affecting the Customer Data. Company's notification regarding or response to a Security Incident under this Section 8 shall not be construed as an acknowledgment by Company of any fault or liability with respect to the Security Incident.

8.2. Company will: (i) take necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) cooperate with the Customer and provide the Customer 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 Customer in writing of any request, inspection, audit or investigation by a supervisory authority or other authority; (iv) keep the Customer informed of all material developments in connection with the Security Incident and execute a response plan to address the Security Incident; and (v) cooperate with the Customer and assist Customer with its obligation to notify the affected individuals in the case of a Security Incident.

9. AUDIT RIGHTS

9.1. Company shall maintain accurate written records of any and all the processing activities of any Personal Data carried out under this DPA and shall make such records available to the Customer and applicable supervisory authorities upon written request. Such records provided shall be considered Company's Confidential Information and shall be subject to confidentiality obligations under the ESA.

9.2. In the event the records and documentation provided subject to Section 9.1 above are not sufficient, Company shall make available, upon at least fifteen (15) days prior written notice, and no more than once per year under the Term and for one year thereafter, to a reputable regional or national auditor nominated by the Customer, 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 Customer Data ("**Audit**") in accordance with the terms and conditions hereunder. The auditor shall be subject to the terms of this DPA and confidentiality obligations of the ESA. Company may object to an auditor appointed by the Customer in the event Company reasonably believes the auditor is not suitably qualified or independent, is a competitor of Company or is otherwise unsuitable ("**Objection Notice**"). The Customer will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from Company. Customer shall bear all costs and 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 Company's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit. Any and all conclusions of such Audit shall be confidential and reported back to Company immediately.

10. TERM & TERMINATION

10.1. This DPA shall be effective as of the Agreement's Effective Date and shall remain in force until the Agreement terminates. The Customer shall be entitled to suspend the Processing of Customer Data in the event the Company is in breach of Data Protection Law, this DPA or a binding decision of a competent court or the competent supervisory authority.

10.2. Company shall be entitled to terminate this DPA or terminate the Processing of Customer Data in the event that Processing of Customer Data under the Customer's instructions or this DPA infringe applicable legal requirements.

10.3. Following the termination of this DPA, Company shall, at the choice of the Customer, delete all Customer Data processed on behalf of the Customer and certify to the Customer that it has done so, or, return all Customer Data to the Customer and delete existing copies, unless applicable law or regulatory requirements requires that Company continue to store Customer Data. Until the Customer Data is deleted or returned, the Parties shall continue to ensure compliance with this DPA.

ANNEX I
DETAILS OF PROCESSING

This Annex includes certain details of the Processing of Personal Data as further described by Article 28(3) GDPR.

Categories of Data Subjects:

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

Categories of Personal Data:

- Recipients:
  - Contact details: Full Name; Email Address; Phone Number
  - Job Title
  - Geographical Location (including home and/or company address)
  - Recipient's behavior segments: emails action (click, open) time of clicking and opening email, email bounce date and email categorize, profiling preference and behavior.

Special Categories of Personal Data:

NA

Nature of the processing:

Processing, hosting and transmission.

Purpose(s) of Processing:

Providing the Services.

Retention Period:

Personal data will be retained for the term of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

Process Frequency:

Continuous basis

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing.

The sub-processors are hosting services, storage providers, and service providers for payment and communication services; the duration of their Processing shall be continuous throughout the term over which Services are used by the Customer.

ANNEX II
TECHNICAL AND ORGANIZATIONAL 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.

Personal Data, whether processed by the Company or for which the Company is deemed the Controller (as such term is defined under the GDPR), is stored by agreement with Cologix, Inc. at one of its New Jersey, USA data centers.

The data processed by the Company as a Processor (as such term is defined under the GDPR) is stored by agreement with Cologix, Inc. at one of its New Jersey, USA data centers. You may review Cologix's resources, security measures and privacy policy via their website at https://cologix.com/. 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 restricted to help ensure that only the relevant personnel who have received prior approval may access the Company's databases. 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. The Company revokes access to Personal Data upon termination of their employment.

Organizational and Operational Security

The Company invests in resources to ensure its security policies and practices are in compliance with law and current market practices, including by providing employees with training with respect to such security policies and practices and consulting with privacy compliance experts. 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 makes commercially reasonable efforts to ensure the transparency of input controls, including the 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.

Data Retention

Personal Data is retained for as long as needed for us to provide the Services or as required by applicable law.

Job Control and Third Party Contractors and Service Providers

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 to help 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.

ANNEX III
LIST OF SUB-PROCESSORS

Name	Location	Description of the processing	Type of Privacy Agreement Executed
Google Analytics	USA	Track usage from visitors and users on the website and applications.	SCC
Impressionwise	USA	Data of website users	GDPR
Mailgun	USA, Germany & Belgium	Email sending and deliverability platform	DPA
Microsoft Teams	USA	Internal communication tool	DPA
Open Text	USA	Data of website users	DPA
SendGrid	USA and Ireland	Email sending and deliverability platform	DPA and BCR
Skype	USA	Internal communication tool	SCC
Sparkpost	USA	Email sending and deliverability platform	DPA
Stripe	USA	Payment processing and payment services	DPA
Xverify	USA	Data cleaning services	DPA
Amazon Web Services	USA	Cloud hosting	SCC
MAPP	USA	Email sending and deliverability platform	DPA

ANNEX IV
CCPA ADDENDUM

In addition to the requirements set forth under this DPA, which shall apply to the collection, processing, use, sharing, sale, and retention of California residents' Personal Information, the obligations set forth under this addendum ("**CCPA Addendum**") shall further apply and are a summary of the Company's CCPA Privacy Notice. All terms used but not defined in this CCPA Addendum shall have the meaning set forth in the CCPA, as amended.

1. For the purposes of the CCPA, Customer is the Business and Company is the Service Provider.
2. Company shall process Personal Information on behalf of the Customer as a Service Provider under the CCPA and shall not sell or share the Personal Information or retain, use or disclose the Personal Information for any purpose other than for Customer purpose specified in the Agreement;
3. Company permits Customer to monitor Company's compliance with this CCPA Addendum subject to Section 9 in the DPA pertaining to "Audit Rights".
4. Company shall notify Customer if Company determines it can no longer meet its obligations under this Addendum or CCPA requirements.
5. Company shall use reasonable efforts to assist Customer in connection with a California resident request to limit the use of the resident's Sensitive Personal Information ("**SPI**"), Company shall provide commercially reasonable assistance, including by coordinating with its sub-contractors, as Customer may reasonably request, where applicable, in connection with Customer obligations to respond to a request for exercising CCPA rights of a California resident.
6. Company shall (a) promptly notify Customer; (b) only act upon a California resident's request with the prior written consent of the Customer; and (c) use commercially reasonable efforts to make available to Customer information which is necessary to demonstrate compliance with the CCPA.
7. Company does not receive or Process any Personal Information as consideration for any Services or other items that Company provides to Customer under the Agreement.
8. Company understands the rules, requirements and definitions of the CCPA and shall refrain from selling (as such term is defined in the CCPA) any Personal Information.