**DATA PROCESSING AGREEMENT**

This Data Processing Agreement ("**DPA**") supplements the master services agreement or any other agreement ("**Agreement**") executed by and between the parties for the purpose of using the Services, as defined under the Agreement.

**WHEREAS**, the Services may require Ongage to Process Personal Data (as such terms are defined below) on the Customer's behalf subject to the terms and conditions of this DPA; and

**WHEREAS**, the parties desire to supplement this DPA to achieve compliance with the UK, EU, Swiss, United States and other data protection laws and agree on the following:

**1. APPLICATION OF THE DPA**

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 Laws. This DPA will only apply to the extent: **(i)** Ongage 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 Laws apply to the processing of Personal Data.
1. In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA.

**2. DEFINITIONS**

2. **"Adequate Country**" is a country that an adequacy decision from the European Commission.
2. "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 -1798.199) of 2018, including as modified by the California Privacy Rights Act ("**CPRA**") once the CPRA takes effect as well as all regulations promulgated thereunder from time to time.
2. "**CPA**" means the Colorado Privacy Act C.R.S.A. § 6-1-1301 et seq. (SB 21-190), including any implementing regulations and amendments.
2. "**CTDPA**" means the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022), including any implementing regulations and amendments thereto.
2. "**Customer Data**" means any and all Personal Data provided by the Customer to Ongage during its use of the Service, as detailed in **Annex I** attached herein.
2. The terms "**Controller**", "**Personal Data**", "**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, CPA , VCDPA, CTDPA. The terms "**Business Purpose**", "**Consumer**", ", "Cross-contextual Advertising", "**Contractor**",, **"First-Party Business",** "**Service Provider**", "**Share**", "**Sale**", "**Targeted Advertising**", "**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 US Data Protection Laws, "**Personal Data**" shall include "**Personal Information**" under this DPA.

2.7. “**Data Protection Law**" means applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws, Israeli Law and the US Data Protection Laws) as may be amended or superseded from time to time.

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

2.9. "**EEA**" means the European Economic Area.

2.10. "**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.

2.11. “**Israeli Law**” means Israeli Privacy Protection Law, 5741-1981, the regulations promulgated pursuant thereto, including the Israeli Privacy Protection Regulations (Data Security), 5777-2017 and other related privacy regulations.

2.12. “**Security Incident**” means any significant accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

2.13. "**Standard Contractual Clauses**" or “**SCC**” 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.

2.14. “**Swiss Data Protection Laws**” or **“FADP”** shall mean (i) Swiss Federal Data Protection Act (dated June 19, 1992, as of March 1, 2019) (“**FDPA**”); (ii) The Ordinance on the Federal Act on Data Protection ("**FODP**"); (iii) any national data protection laws made under, pursuant to, replacing or succeeding and any legislation replacing or updating any of the foregoing.

2.15. “**Swiss SCC”** shall mean the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner.

2.16. ”**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.

2.17. ”**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).

2.18. “**UK Standard Contractual Clauses**” or **“UK SCC**” means the UK “International Data Transfer Addendum to The European Commission Standard Contractual Clauses” available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-tr

ansfer-addendum.pdf as adopted, amended or updated by the UK Information Commissioner Office ("**ICO**"), Parliament or Secretary of State.

2 "**US Data Protection Laws**" means any U.S. federal and state privacy laws effective as of the Effective Date of this DPA and applies to Ongage Processing of Customer Data, and any implementing regulations and amendment thereto, including without limitation, the CCPA, the CPA, the CTDPA, and the VCDPA.

2 "**VCDPA**" means the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq. (SB 1392), including any implementing regulations and amendments thereto.

*Any other terms that are not defined herein shall have the meaning provided under the Agreement or applicable Data Protection Laws. A reference to any term or section of the Data Protection Laws means the version as amended. 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 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, and according to the applicable Data Protection Laws, Ongage 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 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 The Controller acknowledges 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 Additional US Data Protection Laws specifications are further detailed in **Annex VII**.

## 4. PROCESSING OF PERSONAL DATA

4 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, Ongage 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 Ongage and that Ongage 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 Ongage, as well as where applicable, provide the Data Subjects with the ability to opt out.

4 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 Ongage.

- Ongage represents and warrants that it shall Process Customer Data, solely for the purpose of providing the Service, all in accordance with Customer's written instructions including the Agreement and this DPA. Notwithstanding the above, in the event Ongage is required under applicable laws, including Data Protection Law or any union or member state regulation, to Process Customer Data other than as instructed by Customer, Ongage shall make its best efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.
- Ongage shall provide reasonable cooperation and assistance to the Customer in ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of its Customer Data and to consult with the Supervisory Authority (as applicable).
- Where applicable, Ongage shall assist the Customer in ensuring that Customer Data Processed is accurate and up to date, by informing the Customer without delay if it becomes aware of the fact that the CUstomer Data it is Processing is inaccurate or has become outdated.
- Ongage 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 Laws.
- Notwithstanding the above, in the event the Customer is an Israeli establishment or Customer Data includes processing of Israeli data subjects, or in any event that the Israeli Law shall apply, the parties hereby undertake that they comply with the aforesaid regulations as well as comply with the DPA.

**5. DATA SUBJECTS REQUESTS**

- It is agreed that where Ongage receives a request from a Data Subject or an applicable authority in respect of Customer Data Processed by Ongage, Ongage will notify the Customer of such request promptly and 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 Data Protection Law.

**6. SUB-PROCESSING**

6.1. The Customer acknowledges that Ongage may transfer Customer Data to and otherwise interact with third party data processors ("**Sub-Processor**"). The Customer hereby authorizes Ongage 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. Ongage may continue to use those Sub-Processors already engaged by Ongage, 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

Ongage'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, Ongage may, under Ongage's sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise terminate the Agreement.

6.2. Ongage shall, where it engages any Sub-Processor, impose, through a legally binding contract between Ongage e and the Sub-Processor, data protection obligations similar to those set out in this DPA. Ongage 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. Ongage shall remain responsible to the Customer for the performance of the Sub-Processor's obligations in accordance with this DPA. Ongage shall notify the Customer of any failure by the Sub-Processor to fulfill its contractual obligations.

**7. TECHNICAL AND ORGANIZATIONAL MEASURES**

7 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, Ongage hereby confirms that it has implemented and will maintain appropriate physical, technical and organizational measures to protect the Customer Data as required under Data Protection Laws 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 frequent evaluation and regular improvement of outdated security measures.

7 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.

7 The security measures implemented and maintained by Ongage are further detailed in **Annex II**.

**8. PERSONAL DATA SECURITY INCIDENT**

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

8 Ongage will: (i) take necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate 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) co-operate 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 Ongage shall maintain accurate written records of any and all the processing activities of any Customer 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 Ongage's Confidential Information and shall be subject to confidentiality obligations.

9 Customer may audit Ongage compliance with this DPA and Data Protection Laws by requesting a certificate issued for security verification reflecting the outcome of an audit conducted by a third party auditor (e.g., ISO27001 certification) or a comparable certification or other security certification of an audit conducted by a third-party auditor, within 12 months as of the date of Customer's request.

9 Alternatively in the event the records and documentation provided subject to Section 9.1 and 9.2 above are not sufficient for the purpose of demonstrating compliance, Ongage shall make available, solely upon prior reasonable written notice and no more than once per calendar year, to a reputable 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 standard confidentiality obligations (including towards third parties). Ongage may object to an auditor appointed by the Customer in the event Ongage reasonably believes the auditor is not suitably qualified or is a competitor of Ongage. Customer 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 Ongage's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit.

9 Nothing in this DPA will require Ongage either to disclose to Customer or its third-party auditor, or to allow Customer or its third-party auditor to access: any data of any other customer; Ongage's internal accounting or financial information; any trade secret of a Ongage; any information that, in Ongage's reasonable opinion, could compromise the security of any Ongage's systems or cause any breach of its obligations under applicable law or its security or privacy obligations to any third party; or any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Customer's obligations under the Data Protection Laws.

**10. CROSS BORDER PERSONAL DATA TRANSFERS SUBJECT TO GDPR AND FADP**

1 Transfers from the EEA, the UK or Switzerland to non-adequate third countries. Where the GDPR, UK GDPR or the Swiss FADP is applicable, if the Processing of Personal Data by Ongage (or by a Sub-Processor) includes transfer of Personal Data (either directly or through an onward transfer) to a third country outside the EEA, the UK and Switzerland that is not an Adequate Country, such transfer shall only occur if an appropriate safeguard approved by the applicable Data Protection Law (the GDPR (Article 46), UK GDPR (Article 46) or Swiss FADP (as applicable)) for the lawful transfer of Personal Data under is in place.

1 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**").

1. If Ongage or its Sub-processor relies on the Standard Contractual Clauses to facilitate a transfer to a third country that is not an Adequate Country, then:
    1. transfer of Personal Data from the EEA the terms set forth in **Annex IV** shall apply.
    1. transfer of Personal Data from the UK, the terms set forth in **Annex V** shall apply; and
    1. transfer of Personal Data from Switzerland, the terms set forth in **Annex VI** shall apply.

## 11. TERM & TERMINATION

1. This DPA shall be effective as of the Effective Date and shall remain in force until the Agreement terminates or as long as Ongage processes Personal Data. The Customer shall be entitled to suspend the Processing of Customer Data in the event the Ongage is in breach of Data Protection Laws, this DPA or a binding decision of a competent court or the competent supervisory authority.
1. Ongage 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 and Ongage notified the Customer of such infringement and the Customer did not cure such infringement within 10-days. Alternately, Ongage may, in its sole discretion, suspend the processing of the Customer Data until such infringement is cured without terminating the DPA.
1. Following the termination of this DPA, Ongage 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 Ongage 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 under the Data Protection Laws.

***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; all of the above is applicable to the subprocessors

**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.

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). 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.

## SystemControl

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**

| Name | Location | Description of the processing | DPA/SCC Executed |
|---|---|---|---|
| Google Analytics | USA | Track usage from visitors and users on the website and applications. | SCC |
| Amazon Web Services | USA and Ireland | Cloud hosting. | SCC |
| ,Auth0 Inc. (Okta) | Processing region in EU, however, the Headquarters are located in the state of San Francisco, US | Authentication & authorization solution | SCC |
| Digital Ocean | USA | Cloud solutions | SCC |
| .Zendesk Inc | USA | Support Services | SCC |
| Slack Technologies, LLC | USA | Internal communication tool for Support. | SCC |
| ClickaTell | USA | Chat and Communications | Master Terms |
| Jira | USA | Internal task management and correspondence email | DPA |
| SendGrid | USA and Ireland | sending and deliverability platform | DPA & BCR |
| Mailgun | USA, Germany & Belgium | email sending and deliverability platform | DPA |
| MessageBird | USA | email sending and deliverability platform | DPA |
| BlueSnap | US & EEA | Payment Services | DPA |
| Clickhouse | USA | Cloud analytics DB | DPA |
| | | | |
| | | | |
| | | | |
| | | | |

## ANNEX IV

## EU INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to transfer of Personal Data from the EEA to other countries that are not deemed as Adequate Countries.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the transfer is effectuated by Customer as the data controller of the Personal Data and Ongage is the data processor of the Personal Data.
3. The Parties agree that for the purpose of transfer of Personal Data between Customer (as Data Exporter) and the Ongage (as Data Importer), the following shall apply:
   a) Clause 7 of the Standard Contractual Clauses shall not be applicable.
   b) In Clause 9, option 2 (general written authorization) shall apply and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in the Sub-Processing Section of the DPA.
   c) In Clause 11, the optional language will not apply, and data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
   d) In Clause 17, option 1 shall apply. The parties agree that the Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the Customer is established (where applicable).
   e) In Clause 18(b) the parties choose the courts of the Republic of Ireland, as their choice of forum and jurisdiction.

4. **Annex I.A** of the Standard Contractual Clauses shall be completed as follows:

   4.a.1."**Data Exporter**": Customer

   4.a.2."**Data Importer**": Ongage

   4.a.3.Roles: (A) With respect to Module Two: (i) Data Exporter is a data controller and (ii) the Data Importer is a data processor.

   4.a.4.Data Exporter and Data Importer Contact details: As detailed in the Agreement.

   4.a.5.Signature and Date: By entering into the Agreement and DPA, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

5. **Annex I.B** of the Standard Contractual Clauses shall be completed as follows:
   a) The purpose of the processing, nature of the processing, categories of data subjects, categories of personal data and the parties' intention with respect to the transfer of special categories are as described in **Annex I** (Details of Processing) of this DPA.
   b) The frequency of the transfer and the retention period of the personal data is as described in **Annex I** (Details of Processing) of this DPA.
   c) The sub-processor which personal data is transferred are listed in **Annex III**.

6. **Annex I.C** of the Standard Contractual Clauses shall be completed as follows: the competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 3 above.

7. **Annex II** of this DPA (Technical and Organizational Measures) serves as **Annex II** of the Standard Contractual Clauses.

8. **Annex III** of this DPA (List of Sub-processors) serves as **Annex III** of the Standard Contractual Clauses.

**9.** **Transfers to the US:** Measures and assurances regarding US government surveillance ( "**Additional Safeguards**") are further detailed in **Annex II,** as well as:

Ongage agrees and hereby represents it maintains, and will continue to maintain, the following additional safeguards in connection with any Personal Data transferred under this Annex IV:

a) Ongage maintains industry standard measures to protect the Personal Data from interception (including in transit from Customer to Ongageand between different systems and services). This includes maintaining encryption of Personal Data in transit and at rest.
b) Ongage will make reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under the GDPR or the UK GDPR, including (if applicable) under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**").
c) If Ongage becomes aware of any law enforcement agency or other governmental authority ("**Authority**") attempt or demand to gain access to or a copy of the Personal Data (or part thereof), whether on a voluntary or a mandatory basis, then, unless legally prohibited or under a mandatory legal compulsion that requires otherwise, Ongage shall: inform the relevant Authority that Ongage is a Processor of the Personal Data and that Customer, as the Controller has not authorized Ongage to disclose the Personal Data to the Authority; inform the relevant Authority that any and all requests or demands for access to the Personal Data should be directed to or served upon Customer in writing; and use reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Ongage's control.
d) Notwithstanding the above, if, taking into account the nature, scope, context and purposes of the related Authority's intended access to Personal Data, Ongage has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, these subsections shall not apply. In such event, Ongage shall notify Customer, as soon as possible, following the access by the Authority, and provide Customer with relevant details, unless and to the extent legally prohibited to do so.

Ongage will inform Customer, upon written request (and not more than once a year), of the types of binding legal demands for Personal Data Ongage has received and complied with, including demands under national security orders and directives, specifically including any process under Section 702 of FISA.

**ANNEX V**

**EU INTERNATIONAL TRANSFERS AND SCC**

1. The parties agree that the terms of the Standard Contractual Clauses as amended by the UK Standard Contractual Clauses, and as amended in this **Annex V**, are hereby incorporated by reference and shall apply to transfer of Personal Data from the UK to other countries that are not deemed as Adequate Countries.
2. This **Annex V** is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country in reliance on Article 46 of the UK GDPR and with respect to data transfers from controllers to processors or from the processor to its sub-processors.
3. Terms used in this **Annex V** that are defined in the Standard Contractual Clauses, shall have the same meaning as in the Standard Contractual Clauses.
4. This **Annex V** shall (i) be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (ii) not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
5. Amendments to the UK Standard Contractual Clauses:

   5.1. Part 1: Tables

   5.1.1. Table 1 Parties: shall be completed as set forth in Section 4 within **Annex IV** above.

   5.1.2. Table 2 Selected SCCs, Modules and Selected Clauses: shall be completed as set forth in Section 2 and 3 within **Annex IV** above.

   5.1.3. Table 3 Appendix Information: Annex 1A: List of Parties: shall be completed as set forth in Section 2 within **Annex IV** above. Annex 1B: Description of Transfer: shall be completed as set forth in **Annex I** above. Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: shall be completed as set forth in **Annex II** above. Annex III: List of Sub processors: shall be completed as set forth in **Annex III** above.

   5.1.4. Table 4 Ending this Addendum when the Approved Addendum Changes: shall be completed as “neither party”.

**ANNEX VI**

**SUPPLEMENTARY TERMS FOR SWISS DATA PROTECTION LAW TRANSFERS ONLY**

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to Swiss Data Protection Law, and specifically the FDPA:

- The term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.
- The clauses in the DPA protect the Personal Data of legal entities until the entry into force of the Revised Swiss FDPA.
- All references in this DPA to the GDPR should be understood as references to the FDPA insofar as the data transfers are subject to the FDPA.
- References to the "competent supervisory authority", "competent courts" and "governing law" shall be interpreted as Swiss Data Protection Laws and Swiss Information Commissioner, the competent courts in Switzerland, and the laws of Switzerland (for Restricted Transfers from Switzerland).
- In respect of data transfers governed by Swiss Data Protection Laws and Regulations, the EU SCCs will also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws and Regulations until such laws are amended to no longer apply to a legal entity.
- The competent supervisory authority is the Swiss Federal Data Protection Information Commissioner

**ANNEX VII**

**US DATA PROTECTION LAWS ADDENDUM**

This US Privacy Law Addendum ("**US Addendum**") adds specification applicable to US Data Protection Laws . All terms used but not defined in this US Addendum shall have the meaning set forth in the DPA.

**1. CCPA Specifications:**

1. For the purpose of the CCPA, Customer is the Business and Ongage is the Service Provider.
1. Ongage shall process Customer Data on behalf of the Customer as a Service Provider under the CCPA and shall not sell or share the Customer Dataor retain, use or disclose the Customer Data for any purpose other than for Customer purpose specified in the Agreement;
1. Ongage certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from Selling any Customer Data

**2. US Applicable States Specifications:**

2. For the purpose of this US Addendum "Applicable States" shall mean Virginia, California, Colorado, and Connecticut.
2. Ongage agrees to notify the Customer if Ongage makes a determination that it can no longer meet its obligations under this Addendum or US Data Protection Law.
2. Ongage shall provide information necessary to enable the Customer to conduct and document any data protection assessments required by US Data Protection Laws. Notwithstanding the above, Ongage is responsible for only the measures allocated to it.
2. Ongage shall provide assistance and procures that its subcontractors will provide assistance as Customer may reasonably request, where and to the extent applicable, in connection with any obligation by Customer to respond to Consumer's requests for exercising their rights under the US Data Protection Laws Including without limitation, by taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's respective obligation
2. Ongage acknowledges and confirms that it does not any monetary goods, payments or discounts in exchange for processing the Customer Data..
2. Each party shall, taking into account the context of Processing, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The parties are hereby establishing a clear allocation of the responsibilities between them to implement these measures. Ongage technical measures are detailed in the DPA and Annexes above.
2. The Processing instructions, including the nature of Processing, purpose of Processing, the duration of Processing, the type of personal data and the categories of data subjects, are set forth in **Annex I** above.
2. In addition to the Audit rights under Section 9 of the DPA, under US Data Protection Laws and subject to Customer's consent, Ongage my alternately offer, in response to an on premises audit request, initiate a third-party auditor to verify Ongage' compliance with its obligations under this US Data Protection Laws. During such an audit, Ongage will make available to the third-party auditor all information necessary to demonstrate such compliance.

2 Each party will comply with the requirements set forth under US Data Protection Laws with regards to processing of de-identified data, as such term is defined under the applicable US Data Protection Law.

2 When processing Customer Data for the permitted purposes under US Data Protection Laws Ongage shall ensure it complies with applicable laws and shall be liable for such Processing activities.