DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is an agreement between SwanLogic LLC, d/b/a MemberSpace ("**Provider**," "we," "us," or "our") and you or the entity you represent ("**Client**", "you" or "your"). This Agreement supplements the agreement for the operation and management of an electronic authentication and authorization platform for Client and facilitation of payment transactions on Client websites, ("**Services**") previously executed between Client and Provider, as updated from time to time, or other agreement between Client and Provider governing Client's use of the Services (the "**Services Agreement**") when the GDPR or CCPA (as defined below) apply to Provider's processing of Personal Data or Personal Information (as defined below). Unless otherwise defined in this Agreement or in the Services Agreement, all capitalized terms used in this Agreement will have the meanings given to them in Section 2 of this Agreement. In the event of any conflict between this Agreement and any other provision of the Services Agreement with respect to Personal Data, this Agreement shall govern and apply.

1. **Termination.** This Agreement will terminate upon the earliest of: (i) termination of the Services Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination) or (ii) as agreed by the parties in writing. Provider's obligations hereunder shall survive the termination of the Services Agreement until such time Provider no longer has access to, hosts or retains Personal Data or Personal Information.

2. **Definitions.**

"**Client Information**" means any Personal Data Processed by Provider (or a Sub-processor) in the course of providing the Services under the Services Agreement.

"**CCPA**" means California Consumer Privacy Act of 2018, California Civil Code Section 1798.100 et. seq., including all regulations enacted in connection therewith as the same may be amended, supplemented, or replaced from time to time.

"**Consumer**" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by a unique identifier.

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, the GDPR, the CCPA, and in respect of the United Kingdom ("**UK**"), any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the EU, applicable to the Processing of Client Information under the Agreement which are applicable to Client.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Information**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

"**Sub-processor**" means any person (including any third party, but excluding an employee of Provider and employees of any of Provider's sub-contractors) appointed by or on behalf of Processor (or sub-processor) to Process Client Information on behalf of Client under the Agreement.

The terms "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and shall be construed accordingly.

The term "**Consumer**" together with the term "**Data Subject**" will be together defined as "**Individual**" for purposes of this Agreement.

3. Processing of Personal Data or Personal Information.

3.1 Client's Processing of Personal Data or Personal Information.

(a) Client warrants that it has all necessary rights to provide or provide access to the Personal Data or Personal Information to Provider for the Processing to be performed in relation to the Services and shall have sole responsibility for the accuracy, quality, and legality of Personal Data or Personal Information and the means by which Client acquired Personal Data or Personal Information. To the extent required by applicable Data Protection Laws, Client shall provide any necessary notices to Individuals, provide opt-out rights to individuals, and/or obtain consent from Individuals, and shall maintain a record of such notices and/or consents.

(b) Client acknowledges that in connection with the performance of the Services, Provider employs the use of cookies, unique identifiers, and similar tracking technologies ("**Tracking Technologies**"). Client shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as and to the extent are required by Data Protection Laws to enable Provider to deploy Tracking Technologies lawfully on, and collect data from, the devices of Client's end users and process Personal Data or Personal Information in accordance with the Services Agreement and Provider's Privacy Notice. Should such consent be revoked by the Individual (or should an opt-out be exercised), Client is responsible for communicating the fact of such revocation or opt-out to Provider, and Provider remains responsible for implementing any Client instruction with respect to the further processing of that Personal Data or Personal Information.

(c) Client shall, in its use of the Services, Process Personal Data or Personal Information in accordance with the requirements of Data Protection Laws. Client's instructions for the Processing of Personal Data or Personal Information shall comply with Data Protection Laws

3.2 **Roles of the Parties**. For the purposes of this Agreement, when Processing Client Information, Provider is acting as a Data Processor to the extent the GDPR applies and a "Service Provider" to the extent the CCPA applies, Client is a Data Controller to the extent the GDPR applies and a "Business" to the extent the CCPA applies. Provider will engage Sub-processors pursuant to the requirements set forth in Section 5 ("**Sub-processors**"). To the extent Provider processes Personal Data or Personal Information of Client representatives (such as contact information and statistics with respect to use of the Services) to: (i) comply with legal or regulatory obligations applicable to the processing and retention of data to which Provider is subject; (ii) detect and prevent fraud and abuse, (iii) analyze, develop and improve Provider's products and services; and (iv) inform Client of Provider's products and service, Provider is acting as a Data Controller to the extent the GDPR applies and as a "Service Provider" to the extent the CCPA applies with respect to the Processing of Personal Data or Personal Information it receives from Client and accordingly shall process such data in accordance with Provider's Privacy Notice and Data Protection Laws.

3.3 **Client Authority**. Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instructions set forth in Section 3.4 below on behalf of itself. If Client is a Data Processor, Client warrants to Provider that Client's instructions and actions with respect to Client Information, including its appointment of Provider as another Processor or Sub-processor, have been authorized by the relevant Data Controller.

3.4 **Provider's Processing of Client Information**.

(a) To the extent Provider is acting as a Data Processor or Service Provider, Provider shall Process Client Information in accordance with Client's documented instructions, unless Processing is (i) required by applicable laws to which Provider (or the applicable Sub-processor) is subject; (ii) required in response to lawful requests by public authorities; or (iii) carried out in connection with a merger, acquisition, or sale of all or a portion of Provider's assets or in a bankruptcy or liquidation proceeding in which Provider is involved, in which case Provider shall to the extent permitted by applicable laws inform Client of the applicable requirement or contemplated Processing before the relevant Processing of that Client Information.

(b) Client instructs Provider to Process Personal Data or Personal Information to provide the Services in accordance with (i) the Services Agreement (including this Agreement), (ii) any applicable order forms or (iii) any other reasonable instructions provided by Client (e.g., via email or support tickets) that are consistent with the terms of the Services Agreement. Any additional instructions not included in the above shall be subject to the normal change order processes agreed between the parties and may require additional consideration.

(c) Where Provider considers that an instruction infringes applicable Data Protection Laws, it shall immediately inform Client of this, and Client and Provider shall discuss a solution in good faith. Provider will not process the Personal Data subject to the instruction at issue until the Parties agree on a solution. Where Provider is obliged to transfer Personal Data or Personal Information to a third country or an international organization, under Union law or Member State law to which Provider is subject, Provider shall inform Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(d) Client acknowledges that Provider is required under Data Protection Laws to: (i) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Provider is acting and (if applicable) of such processor's or controller's local representative and data protection officer; and (ii) make such information available to the supervisory authorities. Accordingly, Client will, where requested and as applicable to Client, provide such information to Provider by means as may be provided by Provider, and will subject updates to Provider to ensure that all information provided is kept accurate and up-to-date.

(e) Provider will not retain, use or disclose the Client Information for any purpose other than: (i) to process or maintain Client Information on behalf of Client for the purposes set forth in the instructions above; (ii) to retain and employ a Sub-processor, as provided for under Section 5 below; (iii) to detect data security incidents, or protect against fraudulent or illegal activity; or (iv) comply with federal, state, or local laws; (v) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; (vi) to cooperate with law enforcement agencies concerning conduct or activity that Client, Provider, or third party reasonably and in good faith believes may violate federal, state, or local law; or (vii) to exercise or defend legal claims – provided, in all cases, that the use of Client Information for such purposes is carried out only as necessary and in a proportionate manner.

3.5 **Details of the Processing**. The subject-matter of Processing of Client Information by Provider is the performance of the Services pursuant to the Services Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Information and categories of Individuals Processed by Provider as a Data Processor under this Agreement, as required by article 28(3) of the GDPR, are further specified in **Exhibit A** to this Agreement, as may be amended by the parties from time to time. For avoidance of doubt, at no time will the Personal Data or Personal Information Processed by Provider include, national identifiers, passport numbers, social security numbers etc. or any information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation.

4. **Provider Personnel.** Provider shall ensure that the persons authorized to process Personal Data or Personal Information hereunder: (i) are bound by appropriate contractual obligations or are under an appropriate statutory obligation of confidentiality; (ii) process Personal Data or Personal Information only on instructions from Client, unless required to do so by European Union law, Member State law, or other applicable law; (iii) shall not sell Client Information; (iv) shall not retain, use or disclose Client Information outside the direct business relationship between Client and Provider and; (v) have undergone training for the processing of Individual requests and the handling of Personal Information under applicable Data Protection Laws.

5. **Sub-processors.**

5.1 **Appointment of Sub-processors**. For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Information, subject to the provisions of this Section 5.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**. When requested by the Client, Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Information. Client authorizes Provider to engage any Sub-processors listed in **Exhibit B.**

5.3 **Objection Right for New Sub-processors**. Provider shall give Client prior written notice of the appointment of any new Sub-processor. If, within fifteen (15) days of receipt of that notice, Client notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Provider shall make commercially reasonable efforts to change in the provision of the Services in a manner that avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within thirty (30) days from Provider's receipt of Client's notice, notwithstanding anything in the Agreement, Client may, by written notice to Provider, with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 **Sub-processing Agreement; Liability**. Provider has or shall enter into a written agreement with each Sub-processor (the "**Sub-processing Agreement**") containing data protection obligations not less protective than those in this Agreement in particular providing sufficient guarantees to implement appropriate technical and organizational measures with respect to the protection of Client Information to the extent applicable to the nature of the Services provided by such Sub-processor. Client hereby authorizes Provider to enter into the Standard Contractual Clauses with Sub-processor(s) on behalf of Client as attached to this Agreement as **Exhibit D**.

5.5 **Other Sharing**. Client acknowledges that in the provision of the Services, Provider, on receipt of instructions from Client, may transfer or facilitate the transfer of Client Information to and otherwise interact with third parties other than Provider's Sub-processors, as described above. Client agrees that if and to the extent such transfers occur, Client is responsible for entering into separate contractual arrangements with such third parties binding them to comply with obligations in accordance with Data Protection Laws. For avoidance of doubt, such third party data processors are not Sub-processors and Provider shall not bear any responsibility or liability for sharing information with such parties.

6. **Security.** 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, Provider shall in relation to the Client Information implement and maintain throughout the term of this Agreement, the technical and organizational measures set forth in **Exhibit C** (the "**Security Measures**"). Client acknowledges and agrees that it has reviewed and

assessed the Security Measures and deems them to provide a level of security appropriate to the risk in respect of Client Information.

7. **Individual Rights.** Provider will, in a manner consistent with the functionality of the Service, enable Client to: (i) access the Client Information; (ii) rectify inaccurate Client Information; (iii) restrict the processing of Client Information; (iv) delete Client Information; and (v) export Client Information. For the most part, Client may do this accessing a platform connected to the Service. For analytics data or billing data, Client may contact Provider via email at privacy@memberspace.com. If an Individual contacts Provider to exercise the Individual's legal rights under applicable Data Protection Laws, Provider will forward such request to Client without undue delay. Provider may only respond to Individual request after prior written approval by, and on the documented instructions of, Client or as required by laws to which Provider is subject. In such a case, Provider shall, to the extent permitted by applicable laws, inform Client of that legal requirement before responding to the request. If Provider does not respond to the Individual, Provider shall inform that Individual of this fact and direct the individual to make the request with Client. To the extent legally permitted, Client shall be responsible for any costs arising from Provider's provision of such assistance.

8. **Personal Data Breach.**

8.1 **Notification of Personal Data Breach.** Provider shall, to the extent permitted by law, notify Client without undue delay and, where feasible within twenty-four (24) hours after Provider having become aware of a Personal Data Breach affecting Client Information, providing Client with sufficient information and documentation to allow Client to meet any obligations to report or inform Individuals of the Personal Data Breach under the Data Protection Laws.

8.2 **No admission.** Provider's notification of or response to a Personal Data Breach under this Section 8 (Personal Data Breach) will not be construed as an acknowledgement by Provider of any fault or liability with respect to the Personal Data Breach.

9. **Data Protection Impact Assessment and Prior Consultation.** Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Client Information by, and taking into account the nature of the Processing and information available to, Provider.

10. **Return or Destruction of Personal Data or Personal Information.** At Client's election, made by written notice to Provider following thirty (30) days of the date of cessation of any Services involving the Processing of Client Information (the "**Cessation Date**"), Provider shall as soon as reasonably practicable: (i) return a complete copy of all Client Information to Client in such format and manner requested by Client and reasonably acceptable to Provider; and (ii) delete all other copies of Client Information Processed by Provider, except to the extent Provider is required or authorized to retain such Personal Data or Personal Information under the Services Agreement, per a court order, by a regulatory authority or under applicable law . In such cases, the confidentiality obligations and use

restrictions in the Agreement shall continue to apply to such Personal Data or Personal Information and/or copies so retained.

11. **Documentation.** Subject to the provisions of Section 12 below, at Client's written request, Provider shall provide Client with the necessary documentation for demonstrating compliance with Provider's obligations under this Agreement and for allowing Client or any other auditor it has authorized to conduct audits, including inspections, and for contributing to such audits.

12. **Audit.** Provider shall allow Client and Client's authorized representatives to either (i) access and review up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, data protection auditors) or suitable certifications reasonably acceptable to Client to ensure compliance with the terms of this Agreement; or (ii) if the requested audit scope is not addressed the reports listed in (i) above, conduct audits or inspections to ensure compliance with the terms of this Agreement in accordance with this Section 12. Notwithstanding the foregoing, any audit must be conducted during our regular business hours, with reasonable advance notice to Provider and subject to reasonable confidentiality procedures. In addition, audits shall be limited to once per year, unless (a) Provider has experienced a Personal Data Breach within the prior twelve (12) months; (b) an audit reveals a material noncompliance; or (c) otherwise required by Data Protection Laws, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory. To the extent legally permissible, Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

13. **Transfer of Data under the GDPR.**

13.1 **Standard Contractual Clauses**. If the Processing of Personal Data or Personal Information involves the transfer of Personal Data or Personal Information out of the European Economic Area ("**EEA**") or the UK, to countries that do not ensure an adequate level of data protection within the meaning of Data Protection Laws, and such transfers are subject to the Data Protection Laws and do not fall into any exemption under the Data Protection Laws ("**Restricted Transfer**"), Provider shall enter into Standard Contractual Clauses or see to it that another mechanism acceptable under the Data Protection Laws for the cross border transfer is in place in respect of the Restricted Transfer of such Client Information. To the extent executed, such Standard Contractual Clauses shall be incorporated as **Exhibit D** to this Agreement and shall constitute an integral part of it. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.2 **Cooperation; Rights not Affected.** Client undertakes to cooperate as necessary for the implementation of any appropriate mechanism in connection with a Restricted Transfer. Nothing in this Agreement modifies or affects any supervisory authority's or Individual's rights.

14. **Jurisdiction and Governing Law.** The parties to this Agreement hereby submit to the choice of law and jurisdiction stipulated in the Services Agreement with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity, provided, however that: (i) if Standard Contractual Clauses are used in connection with this Agreement, then the parties submit to the law of the European Union Member State in which the data exporter is located and (ii) if there is any conflict with the laws of the European Union member state in which the Client is based, if any, the law of such European

Union member state would prevail only with respect to the sections concerning which there is such conflict.

[Remainder of Page Intentionally Left Blank; Signature Pages to Follow]

EXECUTED by and on behalf of:
Provider
....
Name: Ward Sandler
Role: CEO
Date: July 18, 2022

EXECUTED by and on behalf of
....
....
Name:
Role:
Date:

EXHIBIT A TO DATA PROCESSING AGREEMENT: DETAILS OF PROCESSING

- **Duration of the Processing**: The duration of data processing is for the duration of the Services Agreement, plus the period following the expiration of the Services Agreement until Personal Data or Personal Information is deleted

- **Nature and Purpose of the Processing**: The scope and purpose of processing of the Individuals' Personal Data or Personal Information is to facilitate the provision of Provider's Services.

- **Types of Client Information:** The Personal Data or Personal Information includes e-mail, name, IP address, documents and other data in an electronic form provided in the context of Provider's Services, which shall not include any national identifiers, passport numbers, social security numbers etc. or any information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation.

- **Categories of Individuals:** Individuals include the Client's representatives and end users including employees, contractors, collaborators, and Client's customers. Individuals may also include individuals attempting to communicate or transfer personal information to users of Provider's Services. The Individuals exclusively determine the content of data submitted to Provider.

EXHIBIT B TO DATA PROCESSING AGREEMENT: LIST OF SUB-PROCESSORS

See: https://www.memberspace.com/privacy/sub-processors

EXHIBIT C TO DATA PROCESSING AGREEMENT: SECURITY CONTROLS

Provider has implemented and will maintain and follow for online services the following security measures, Provider's only responsibility with respect to the security of Client Information.

Domain	**Practice**
Organization of Information Security	**Security Ownership**. Provider has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. (Ryan Bennick) **Security Roles and Responsibilities**. Provider personnel with access to Client Information are subject to confidentiality obligations. **Risk Management Program**. Provider will perform an internal security audit and review its policies and procedures once a year.
Asset Management	**Asset Inventory**. Provider maintains an inventory of all media on which Client Information is stored. Access to the inventories of such media is restricted to Provider personnel authorized in writing to have such access. **Asset Handling** - Provider imposes restrictions on printing Client Information and has procedures for disposing of printed materials that contain Client Information. - Provider personnel must obtain Provider authorization prior to storing Client Information on portable devices or remotely accessing Client Information.
Human Resources Security	Provider informs its personnel about relevant security procedures and their respective roles. Provider also informs its personnel of possible consequences of breaching the security rules and procedures.
Physical and Environmental Security	Provider personnel does not have access to any physical systems. All of these systems are maintained by 3rd party providers such as AWS.

Communications and Operations Management	**Operational Policy**. Provider maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Information. **Data Beyond Boundaries** - Provider encrypts, or enables Client to encrypt, Client Information that is transmitted over public networks.
Access Control	**Access Policy**. Provider maintains a record of security privileges of individuals having access to Client Information. **Access Authorization** - Provider maintains and updates a record of personnel authorized to access Provider systems that contain Client Information. - Provider deactivates authentication credentials that have not been in use for six months or more. - Provider identifies those personnel who may grant, alter or cancel authorized access to data and resources. **Least Privilege** - Technical support personnel are only permitted to have access to Client Information when needed. - Provider restricts access to Client Information to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Provider stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Provider uses encrypted protocols to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Provider requires the password to be at least eight characters long.

	- Provider does not reallocate de-activated or expired identifiers. - Provider uses a one way password hashing function on passwords that are stored at rest in our database. When authenticating users we compare the results of the hashing algorithm. We incorporate a salt to protect against rainbow table attacks and brute-force search attacks.
Information Security Incident Management	- Provider maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - In the event of a security breach which constitutes a Personal Data Breach as defined in the European Data Protection Regulation (GDPR) affecting Client Information, we will notify our Client without undue delay and, where feasible, within 24 hours after having become aware of the Personal Data Breach.
Data Recovery Procedures	- On an ongoing basis Provider maintains multiple copies of Client Information from which Client Information can be recovered. - Provider stores copies of Client Information and data recovery procedures in a different place from where the primary computer equipment processing the Client Information is located. - Provider reviews data recovery procedures at least every six months.

EXHIBIT D – MODEL CONTRACTUAL CLAUSES

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……………………………………………………………
(the data **exporter**)

And
Name of the data importing organisation: SwanLogic LLC, d/b/a MemberSpace

Address: 625 Washington Street, Hoboken, NJ 07030

Tel.: 908-304-3859; e-mail: privacy@memberspace.com

Other information needed to identify the organisation:

………………………Not Applicable……………………………………
(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

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

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

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

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

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

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

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

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

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

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

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

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

(ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12

Obligation after the termination of personal data processing services

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

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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

Clarifications to the Standard Contractual Clauses: The parties agree that:

1. The audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the provisions of Section 12 above.

2. The certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Provider to the Client upon Client's request.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……Walsh………………………………….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is ____.

Data importer

The data importer is SwanLogic LLC, d/b/a MemberSpace.

- **Types of Client Information:** The personal data transferred includes e-mail, name, IP address, documents and other data in an electronic form provided in the context of Provider's Services, which shall not include any national identifiers, passport numbers, social security numbers etc . or any information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation.

Categories of Data Subjects: Data subjects include the Client's representatives and end users including employees, contractors, collaborators, and Client's customers. Data subjects may also include individuals attempting to communicate or transfer personal information to users of Provider's Services. The data subjects exclusively determine the content of data submitted to Provider.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

A. **Duration and Object of Data Processing**. The duration of data processing is for the duration of the Services Agreement, plus the period following the expiration of the Services Agreement until Personal Data is deleted. The objective of the data processing is the performance of the Services.

B. **Scope and Purpose of Data Processing**. The scope and purpose of processing personal data is to facilitate provision of the Services.

C. **Customer Data Access**. Shall be as set forth in Section 9 of the Agreement

D. **Data Exporter's Instructions**. Shall be as set forth in Section 3.4 of the Agreement

E. **Customer Data Deletion or Return**. Shall be as set forth in Section 10 of the Agreement

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

See Exhibit B to Agreement