Sharecare, Inc. Vendor Data Processing Addendum

This Data Addendum ("DPA") forms an integral part of the Services Agreement ("Agreement") between Sharecare, Inc. ("**Sharecare**") and the vendor identified in the Agreement ("**Vendor**") and applies to the extent that Vendor processes Personal Data on behalf of Sharecare in the course of providing Services under the Agreement.

Recitals

(1) As part of its privacy policy and its contractual arrangements, Sharecare is committed to ensuring the appropriate protection of Personal Data of persons protected by Applicable Privacy Law(s) whose data is processed by Sharecare, including but not limited to those identified in Appendix 1 of Annex A hereto ("Data Subjects").

(2) Sharecare's commitment to Personal Data protection continues when Sharecare engages third party Vendors, including but not limited to, Service Providers as defined by the CCPA.

(3) Accordingly, the parties desire to amend and supplement the Agreement as set forth herein.

(4) Sharecare's engagement of Vendor is conditioned upon Vendor's agreement to the terms and conditions of this DPA.

Agreement

1. Definitions

1.1 "**Affiliate(s)**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

1.2 "**Applicable Privacy Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Processing of Personal Data pursuant to the Agreement, including, where applicable, local, state, national and/or foreign laws including, but not limited to, CCPA and EU Data Protection Law and implementations of EU Data Protection Law into national law.

1.3 "**Authorized Persons**" means any person who processes Personal Data on Vendor's behalf, including Vendor's employees, officers, partners, principals, contractors and Subcontractors.

1.4 **"Controller"** means an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Sharecare is the Controller.

1.5 **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 *et seq.,* including any amendments and any implementing regulations thereto that become effective before, on or after the effective date of this Data Processing Addendum.

1.6 **"CCPA Consumer"** means a "consumer" as such term is defined in the CCPA.

1.7 **"Data Processor" or "Processor" or "Subprocessor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable but not limited to any "Service Provider" as that term is defined by the CCPA.

1.8 "**EEA**" means, the European Economic Area.

1.9 "**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data ("**Directive**") and all applicable member state implementations thereof; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") and all applicable member state implementations thereof.

1.10 **"EU Model Clauses"** means the standard contractual clauses for Processors as approved by the European Commission pursuant to Decision C (2010) 593, as they may be amended or replaced from time to time.

1.11 "**Personal Data**" means any information and data, including but not limited to Personal Information as defined by the CCPA, submitted to Vendor by Sharecare relating to i) an identified or identifiable natural person ("Data Subject"); or ii) an identified or identifiable legal entity, where such information is protected similarly as personal data under Applicable Privacy Laws. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, Personal Data includes personally identifiable information.

1.12 "**Personal Information**" shall have the meaning set forth in the CCPA.

1.13 "**Privacy Shield**" means, collectively, the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2016) 4176 dated July 12, 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

1.14 "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive.

1.15 "**Processing" or "Process**" or **"Data Processing"** means any operation or set of operations performed on Personal Data or sets of Personal Data as defined in Art. 2(b) Data Protection Directive and Art. 4(2) GDPR or any operation or set of operations that are performed on Personal Information as defined by Cal. Civ. Code § 1798.140(o), such as but not limited to collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

1.17 "**Security Incident**" means any breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure or access to, Personal Data.

1.18 **"Service(s)"** means work that Vendor performs for Sharecare as described in the Agreement.

1.19 **"Service Provider"** is defined by Cal. Civ. Code § 1798.140(v) and means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of Sharecare and to which Sharecare discloses a CCPA Consumer's Personal Information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the Personal Information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the services specified in the contract with the business.

1.20 "**Subcontractor**" means any third party (including but not limited to any Vendor affiliates) engaged directly or indirectly by Vendor as a subprocessor to process any Personal Data relating to this DPA and/or the Agreement. The term "Subcontractor" shall also include any third party appointed by a Subcontractor to process any Personal Data relating to this DPA and/or the Agreement.

1.21 **"Valid Transfer Mechanism"** means a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside the EEA.

2. Data Processing: Role, Scope, and Instructions for Processing

2.1 **Scope and Roles.** This DPA applies when Personal Data is processed by Vendor. In this context, Vendor will act as Data Processor to Sharecare, who will act as Controller with respect to Personal Data (as each term is defined in Section 1).

2.2 **Subject-Matter. Nature, Purpose, and Duration of Data Processing.** The subject matter of the Data Processing under this DPA is Personal Data. The nature of the processing will include computing, storage, and such other Services as described in the Agreement. The purpose of the Data Processing under this DPA is the provision of the Services by Vendor pursuant to the Agreement. The type of Personal Data and categories of Data Subjects are determined by the Agreement and may include but are not limited to Sharecare's customers, employees, suppliers, and end-users. The duration of Processing Personal Data shall be for the term of the Agreement. Vendor shall not retain, use or disclose Personal Information for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by the CCPA. Vendor acknowledges and agrees that it shall not retain, use or disclose Personal Information for a commercial purpose other than providing the Services. Processing Personal Data outside the scope of this DPA or the Agreement will require prior written agreement, with additional instructions for Processing, between Sharecare and the Vendor.

2.3 **Documented Instructions.** Vendor will at all times: (i) process the Personal Data only in accordance with Sharecare's documented instructions and in accordance with the Agreement; (ii) not process the Personal Data for its own purposes or those of any third party; (iii) not disclose, release, transfer, make available or otherwise communicate any Personal Information to another business or third party without the prior written consent of Sharecare unless and to the extent that such disclosure is made to a Subprocessor for a business purpose, provided that Vendor has entered into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Personal Information as are imposed on the Vendor under this DPA and the Agreement; and (iv) not sell any Personal Data to another business or third party without the prior written consent of Sharecare. Notwithstanding the foregoing, nothing in this Agreement shall restrict the Vendor's ability to disclose Personal Data to comply with applicable laws. Each Party shall comply with its obligations under Applicable Privacy Law(s) in respect of any Personal Data it Processes under this DPA.

2.4 **Valid Transfer Mechanism.** If Vendor Processes Personal Data outside the EEA or countries formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries") it will do so pursuant to a Valid Transfer Mechanism for all Personal Data transferred out of the EEA and/or Switzerland.

3. Personnel and Sub-processing

3.1 Vendor shall take reasonable steps to require screening of its personnel who may have access to Personal Data, and shall ensure its personnel (i) Process Personal Data in accordance with Sharecare's instructions as set forth in the Agreement and with Applicable Privacy Law(s); (ii) receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and, (iii) are subject to confidentiality obligations which shall survive the termination of employment.

3.2 Vendor shall not subcontract any processing of the Personal Data to a Subcontractor without the prior written consent of Sharecare. Notwithstanding the foregoing, Sharecare consents to Vendor changing or adding to the

Subcontractors listed in **Annex B**, which is incorporated by reference herein, to process the Personal Data provided that:

(a) Vendor provides prompt written notice to Sharecare of the engagement of any new Subcontractor (including details of the processing and location), and Vendor shall update the list of all Subcontractors engaged to process Personal Data under this Agreement at **Annex B** and send such updated version to Sharecare prior to the engagement of the Subcontractor;

(b) Vendor imposes the same data protection terms on any Subcontractor it engages as contained in this DPA (including but not limited to the Privacy Shield Principles and/or other Valid Transfer Mechanism provisions, where applicable), providing sufficient guarantees to implement appropriate technical and organisational measures to meet Applicable Privacy Laws and ensuring that such Subcontractor has entered into a written agreement requiring the Subcontractor to abide by terms no less protective than those provided in this DPA; and

(c) Vendor remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subcontractor.

3.3 If Sharecare objects to the engagement of any Subcontractor on data protection grounds, then either Vendor will not engage the Subcontractor to process the Personal Data or Sharecare may elect to immediately suspend or terminate the processing of Personal Data under the Agreement(s) and/or immediately suspend or terminate the Agreement(s), in each case without penalty. Upon any termination by Sharecare pursuant to this Section, Vendor shall refund Sharecare any prepaid fees for the terminated portion(s) of the Services that were to be provided after the effective date of termination.

4. Cooperation

4.1 Vendor shall comply with Applicable Privacy Laws by assisting and reasonably cooperating with Sharecare to enable Sharecare (or its third party Controller) to respond to any i) Data Subject requests for access, correction, deletion or restriction of that person's Personal Data ("Data Subject Request") or CCPA Consumer requests as governed by applicable CCPA requirements; and ii) complaints or other communications from Data Subjects and governmental, regulatory or judicial bodies relating to the processing of Personal Data under the Agreement(s), including but not limited to requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws, in which case Vendor will either (i) provide Sharecare with the ability within the Services to correct or delete Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Sharecare's behalf if such functionality is not available within the Services. In the event that any such Data Subject Request or CCPA Consumer request, complaint, or communication is made directly to Vendor, Vendor shall immediately notify and pass this onto Sharecare and shall not respond to such communication without Sharecare's express authorization. During the term of the Agreement, Vendor shall ensure that Sharecare can extract Personal Data from the Services in a structured, commonly used and machine-readable format such that Sharecare can provide the Personal Data to an individual who makes a data portability request under EU Data Protection Laws.

4.2 If Vendor receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Personal Data, Vendor shall not disclose any information but shall immediately notify Sharecare in writing of such request, and reasonably cooperate with Sharecare if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

4.3 To the extent Vendor is required under Applicable Privacy Laws, Vendor will assist Sharecare (or its third party Controller) to conduct a data protection impact assessment and, where legally required, consult with applicable data protection authorities in respect of any proposed processing activity that present a high risk to data subjects.

5. Data Access & Security Measures

5.1 Vendor shall ensure that any Authorized Person is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services under the Agreement to Sharecare.

5.2 Vendor will implement and maintain all appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of Personal Data ("**Security Measures**"). Such measures shall have regard for 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. At a minimum, Vendor agrees to the Security Measures identified at **Appendix 2 of Annex A hereto**. Vendor shall, to the extent possible, use best in class encryption technologies for transmitting and storing Personal Data. Vendor shall also employ best in class network security techniques, including but not limited to, firewalls, intrusion detection, and authentication protocols.

6. Security Incidents

6.1 In the event of a Security Incident, Vendor shall promptly (and in no event later than 48 hours of becoming aware of such Security Incident) inform Sharecare and provide written details of the Security Incident, including but not limited to the type of data affected and the identity of affected person(s) or legal entities as soon as such information becomes known or available to Vendor.

6.2 Furthermore, in the event of a Security Incident, Vendor shall:

(a) Include in the notification, to the extent known at the time of notification, (i) a description of the Security Incident, including but not limited to, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the name and contact details of Vendor's data protection officer or other contact point where more information can be obtained; (iii) a description of the likely consequences of the Security Incident; and (iv) a description of the measures taken or proposed to be taken by Vendor to address the Security Incident, including but not limited to, where appropriate, measures to mitigate its possible adverse effects. If Vendor is unable it is to provide all of the information listed above as part of the initial notification, Vendor will provide this information to Sharecare as soon as reasonably practicable. To the extent Sharecare requires additional information from Vendor to meet its Security Incident notification obligations under applicable Data Protection Laws, Vendor shall provide reasonable assistance to provide such information to Sharecare taking into account the nature of Processing and the information available to Vendor;

(b) provide timely information and cooperation as Sharecare may require to fulfil Sharecare's data breach reporting obligations under Applicable Privacy Laws; and

(c) take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep Sharecare up-to-date about all developments in connection with the Security Incident.

6.3 The content and provision of any notification, public/regulatory communication, or press release concerning the Security Incident shall be solely at Sharecare's discretion, except as otherwise required by applicable laws.

7. Security Reports & Inspections

7.1 Upon request, Vendor shall provide copies of relevant external certifications, audit report summaries and/or other documentation reasonably required by Sharecare to verify Vendor's compliance with this DPA.

7.2 While it is the parties' intention ordinarily to rely on Vendor's obligations set forth in Section 7.1 to verify Vendor's compliance with this DPA, Sharecare (or its appointed representatives) may carry out an inspection of the Vendor's operations and facilities during normal business hours and subject to reasonable prior notice where Sharecare considers it necessary or appropriate.

8. International Transfers

8.1 Vendor will at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Applicable Privacy Laws.

8.2 Vendor shall not process or transfer any Personal Data in or to a territory other than the territory in which the Personal Data was first collected (nor permit the Personal Data to be so processed or transferred) unless: (i) it has first obtained Sharecare's prior written consent; and (ii) it takes all such measures as are necessary to ensure such processing or transfer is in compliance with Applicable Privacy Laws (including but not limited to such measures as may be communicated by Sharecare to Vendor) and this DPA.

8.3 Vendor and its Subcontractors have self-certified compliance with the US-EU and US-Swiss Privacy Shield Framework ("Privacy Shield") to protect Personal Data that is transferred to Vendor and its Subcontractors.

8.4 Where Vendor processes Personal Data under this DPA that originates from the EEA, Vendor shall:

(a) provide at least the same level of protection to such Personal Data as is required by the Privacy Shield Principles and/or as Sharecare may otherwise reasonably require to ensure an adequate level of protection for such Personal Data in accordance with the requirements of Applicable Privacy Laws;

(b) comply with Annex A hereto, containing EU Model Clauses, if Personal Data is to be transferred outside the EEA;

(c) promptly notify Sharecare if it makes a determination that it can no longer meet its obligations under Section 8.2 above, and in such event, work with Sharecare and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by Applicable Privacy Laws via an alternative Valid Transfer Mechanism; and

(d) immediately cease (and require that all Subcontractors to immediately cease) processing such Personal Data if in Sharecare's sole discretion, Sharecare determines that Vendor has not or cannot correct any non-compliance with Section 8.3(a) above in accordance with Section 8.3(c) within a reasonable time frame.

8.5 If at any time Vendor or its Subcontractor no longer participate in the Privacy Shield, Vendor and its Subcontractors shall notify Sharecare in accordance with the notice provisions set forth in this Agreement, at which time Sharecare and Vendor will mutually agree upon additional contractual measures, if any, that may be needed to comply with all Applicable Privacy Laws.

9. Deletion & Return

9.1 Upon Sharecare's request, or upon termination or expiration of this DPA or the Agreement or termination of the Services for whatever reason, Vendor shall promptly destroy all Personal Data (including copies) in its possession or control (including but not limited to any Personal Data processed by its Subcontractors). This requirement shall not apply to the extent that Vendor is required by any applicable law to retain some or all of the Personal Data, in which event Vendor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

10. General

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA controls and takes precedence. With effect from the effective date, this DPA is part of, and incorporated into the Agreement.

10.2 The obligations placed upon the Vendor under this DPA shall survive so long as Vendor and/or its Subcontractors process Personal Data on behalf of Sharecare.

10.3 The parties acknowledge and agree that any breach by Vendor of this DPA shall constitute a material breach of the Agreement, in which event and without prejudice to any other right or remedy available to it, Sharecare may elect to immediately terminate the Agreement in accordance with the termination provisions in the Contract(s).

10.4 In the event there is any act or omission (whether grossly negligent, reckless, intentional, or otherwise) on the part of the Vendor and/or its Subcontractors in connection with the activities contemplated by this DPA which leads to Sharecare or its Subsidiaries being liable for breaches of Applicable Privacy Laws or any third party contract, then Vendor shall indemnify Sharecare, its Subsidiaries and their respective officers, directors, employees or agents for any and all damages, fines, penalties, losses, liabilities, costs, harm or expenses (including reasonable legal fees) suffered by Sharecare as a result.

10.5 This DPA may not be modified except by a subsequent written instrument signed by both parties.

10.6 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

10.7 This DPA may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may execute and deliver signatures to this DPA electronically, including by facsimile or portable document format file (PDF).

Annex A- Model 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,

Sharecare, Inc.,

with a principal address of 255 E. Paces Ferry Road, Suite 700, Atlanta, GA, 30305, USA (the "**data exporter**"),

and

the entity identified as "Vendor" in the DPA (the "**data processor/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.

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 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.

---

[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, defense, 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 recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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.

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.

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.

Appendix 1 to the Standard Contractual Clauses

Details of the Processing

Description of Controller/Data Exporter and Data Importer:

The data exporter is Sharecare, Inc.

The data importer is the entity identified as “Vendor” in the Agreement.

As between Sharecare, Inc. and Vendor, Sharecare shall be the Controller of certain Personal Data provided to Vendor to provide the Services.

Type(s) and Categories of Personal Data processed:

The personal data is defined in Section 2.2 of the DPA.

Categories of Data Subjects:

Data subjects are defined in Section 2.2 of the DPA.

Scope and Purpose of the Processing

The processing operations are defined in Section 2.2 of the DPA.

Appendix 2

Sharecare Vendor Information Security Addendum, as executed by the Parties, is incorporated by reference as if fully set forth herein.

Annex B- List of Vendor's Subcontractors

[**Vendor to list all Subcontractors here (including any and all Vendor affiliates processing Personal Data).**]

Name	Nature of Processing	Territory(ies)
E.g: Adobe Analytics	E.g. Analytics for marketing and forecasting.	