DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Agreement between the party identified in the Agreement ("**Customer**") and CareAR, and applies to the extent that (i) CareAR processes Personal Data on behalf of Customer in the course of providing Services, and (ii) the Agreement expressly incorporates this DPA by reference. This DPA does not apply where CareAR is the Controller. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

DEFINITIONS.

1.1 **"Agreement"** means the agreement and/or terms of service between Customer and CareAR for the provision of the Services to Customer.

1.2 **"Controller"** means an entity that determines the purposes and means of the processing of Personal Data.

1.3 **"Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

1.4 **"GDPR"** means 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).

1.5 **"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by CareAR in connection with the provision of the Services under the Agreement.

1.6 **"Personal Data Breach"** means a breach of security in the provision of the Services resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.7 **"Processor"** means an entity that processes Personal Data on behalf of a Controller.

1.8 **"Services"** means any Services provided by CareAR to Customer pursuant to the Agreement.

1.9 **"Sub-processor"** means any third party Processor engaged by CareAR that processes Personal Data pursuant to the Agreement.

2. PROCESSING.

2.1 **Role of the Parties**. As between CareAR and Customer, CareAR will process Personal Data under the Agreement only as a Processor acting on behalf of the Customer. Customer is the Controller with respect to all such Personal Data.

2.2 **Customer Processing of Personal Data**. Customer will, in its use of the Services, comply with its obligations under Data Protection Laws in respect of its processing of Personal Data and any processing instructions it issues to CareAR. Customer represents that it has all rights and authorizations and has provided/obtained all legally required notices/consents necessary for CareAR to process Personal Data pursuant to the Agreement.

2.3 CareAR Processing of Personal Data.

2.3.1 CareAR will comply with Data Protection Laws applicable to its provision of the Services, and will process Personal Data in accordance with Customer's documented instructions. Customer agrees that the Agreement is its complete and final instructions to CareAR in relation to the processing of Personal Data. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between CareAR and Customer by way of written amendment to the Agreement, and will include any additional fees that may be payable by Customer to CareAR for carrying out such instructions. Upon notice in writing, Customer may terminate the Agreement if CareAR declines to follow Customer's reasonable instructions that are outside the scope of, or changed from, those given or agreed to in the Agreement, to the extent such instructions are necessary to enable Customer to comply with Data Protection Laws.

2.3.2 Without limiting the generality of the foregoing, to the extent the California Consumer Privacy Act of 2018, as amended, Cal. Civ. Code § 1798.100 *et.seq.* ("**CCPA**"), applies to any Personal Data, such Personal Data will be disclosed by Customer to CareAR for a 'business purpose' and CareAR will act as Customer's 'service provider', as such terms are defined under CCPA. CareAR will not sell, rent, lease, release, retain, use or disclose Personal Data for a commercial purpose other than for the specific purpose of providing the Services, as further described in the Agreement, or as otherwise permitted by the CCPA.

2.4 Processing of Personal Data Details.

2.4.1 Subject matter. The subject matter of the processing under the Agreement is the Personal Data.

2.4.2 Duration. The duration of the processing under the Agreement is determined by Customer and as set forth in the Agreement and will extend for the duration of the Agreement.

2.4.3 Purpose. The purpose of the processing under the Agreement is the provision of the Services by CareAR to Customer as specified in the Agreement.

2.4.4 Nature of the processing. CareAR and/or its Sub-processors are providing Services or fulfilling contractual obligations to Customer as described in the Agreement. These Services may include the processing of Personal Data by CareAR and/or its Sub-processors on systems that may contain Personal Data.

2.4.5 Categories of data subjects. Customer determines the data subjects which may include Customer's end users, employees, contractors, suppliers, and other third parties.

2.4.6 Categories of data. Personal Data that Customer submits to the Services, namely:

First and Last Names
Email Addresses
Telephone numbers (at user's discretion)
User's Profile Photos (at user's discretion)
GPS coordinates (at user's discretion)
IP Address

3. SUBPROCESSING.

3.1 **Use of Sub-Processors**. CareAR engages Sub-processors to provide certain services on its behalf. Customer consents to CareAR engaging Sub-processors to process Personal Data under the Agreement. CareAR will be responsible for any acts, errors, or omissions of its Sub-processors that cause CareAR to breach any of CareAR's obligations under this DPA.

3.2 **Obligations.** CareAR will enter into an agreement with each Sub-processor that obligates the Sub-processor to process the Personal Data in a manner substantially similar to the standards set forth in the DPA, and at a minimum, at the level of data protection required by Data Protection Laws (to the extent applicable to the services provided by the Sub-processor).

3.3 **Notice.** A list of CareAR Sub-processors is posted at http://carear.com/gdpr-subprocessors.

3.4 **Changes to Sub-processors.** CareAR agrees (i) to provide prior notice to Customer of any new engagement of a Sub-processor to process Personal Data if the Customer has subscribed to receive notification via the mechanisms that CareAR provides for the specific Service; and (ii) if Customer objects to a new Sub-processor on reasonable data protection grounds within ten (10) days of receiving the notice, to discuss with Customer those concerns in good faith with a view to achieving resolution.

4. SECURITY MEASURES.

4.1 **Security Measures by CareAR.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Personal Data and Processing activities, CareAR will implement and maintain appropriate physical, technical and organizational security measures to protect against Personal Data Breaches and to preserve the security, accuracy and confidentiality of Personal Data processed by CareAR on behalf of Customer in the provision of the Services (**"Security Measures"**). The Security Measures are subject to technical progress and development. CareAR may update or modify the Security Measures from time to time provided that any updates and modifications do not result in material degradation of the overall security of the Services purchased by the Customer.

4.2 **Security Measures by Customer.** Customer is responsible for using and configuring the Services in a manner that enables Customer to comply with Data Protection Laws, including implementing appropriate technical and organizational measures.

4.3 **Personnel.** CareAR restricts its personnel from processing Personal Data without authorization (unless required to do so by applicable law) and will ensure that any person authorized by CareAR to process Personal Data is subject to an obligation of confidentiality.

4.4 **Prohibited Data.** Customer acknowledges and agrees that the Services are not intended to process special category or highly sensitive Personal Data (such as an individual's financial or health information, race or ethnicity, etc.) and Customer shall not enter any such data into the Services or an associated application.

5. PERSONAL DATA BREACH RESPONSE.

Upon becoming aware of a Personal Data Breach, CareAR will investigate the cause of the incident, notify Customer promptly and without undue delay and will provide non-privileged, non-confidential, non-proprietary information relating to the Personal Data Breach as reasonably requested by Customer. CareAR will use reasonable efforts to assist Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

6. AUDIT REPORTS.

CareAR audits its compliance against data protection and information security standards on a regular basis. Upon Customer's written request, and subject to obligations of confidentiality, within thirty (30) business days of such a request and no more than once per calendar year, CareAR will make available to Customer a summary of its most recent relevant audit report and/or other documentation reasonably required by Customer which CareAR makes generally available to its customers, so that Customer can verify CareAR's compliance with this DPA.

7. DATA TRANSFERS AND EXPORTS.

7.1 **Data Transfers.** CareAR may transfer and process Personal Data to and in other locations around the world where CareAR or its Sub-processors maintain data processing operations as necessary to provide the Services as set forth in the Agreement.

7.2 **Data Transfers from the EEA, UK and Switzerland.** The parties acknowledge that CareAR transfers data to third countries pursuant to the Standard Contractual Clauses attached hereto.

7.3 **Standard Contractual Clauses.** This DPA hereby incorporates by reference the Standard Contractual Clauses ("SCCs") for data controller to data processor transfers approved by the European Commission pursuant to the GDPR, and which are attached to this Agreement as Schedule 1. The Parties agree that the SCCs will apply to Personal Data that is transferred from the EEA, UK and Switzerland to outside of these geographies, and specifically, either directly or via onward transfer, to the United States. Data Controller/Customer's and Data Processor/CareAR's execution of the Agreement shall be deemed their execution of this DPA and the SCCs, and they thereby acknowledge that (i) Data Controller is the "data exporter" and Data Processor is the "data importer," and (ii) Schedule 1 and the attachments and annexes thereto constitute the SCCs applicable to Personal Data under the Agreement.

8. DELETION OF DATA.

Following expiration or termination of the Agreement, CareAR will delete or (if requested by Customer and required by law) return to Customer all Personal Data in CareAR's possession as set forth in the Agreement except to the extent CareAR is required by applicable law to retain some or all of the Personal Data (in which case CareAR will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to that retained Personal Data.

9. COOPERATION.

9.1 **Data Protection Requests.** If CareAR receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under Data Protection Laws, where CareAR is able to associate the data subject with Customer, CareAR will promptly redirect the request to the Customer. In such case, CareAR will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If CareAR is required to respond to such a request, CareAR will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.

9.2 **Customer Requests.** CareAR will reasonably cooperate with Customer, at Customer's expense, to permit Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. Customer shall first use reasonable endeavours to access the relevant Personal Data in their use of the Services, to facilitate their response.

9.3 **DPIAs and Prior Consultations.** To the extent required by Data Protection Laws, CareAR will, upon reasonable notice and at Customer's expense, provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments (**"DPIAs"**) and/or prior consultations with data protection authorities.

9.4 **Legal Disclosure Requests.** If CareAR receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, it will notify all pertinent parties of such action (a) that as between the parties, the Personal Data requested is Customer's sole property, and (b) Customer is solely responsible for the disposition of such Personal Data including in response to such request. Where legally permissible, CareAR will promptly notify Customer and provide Customer with a copy of the request.

10. GENERAL.

10.1 **Relationship with Agreement.** Any claims brought under this DPA against CareAR will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

10.2 **Conflicts.** In the event of any conflict between this DPA and any privacy-related provisions in the Agreement, the terms of this DPA will prevail. The SCCs shall prevail over the body of this DPA in the event of a conflict.

10.3 **Modification and Supplementation.** CareAR may modify the terms of this DPA as provided in the Agreement, in circumstances such as (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Data Protection Laws, or (iii) to implement or adhere to updated standard contractual clauses, approved codes of conduct or certifications, or other compliance mechanisms, which may be made or permitted under Data Protection Laws. Supplemental terms may be added as an Annex or Appendix to this DPA where such terms only apply to the processing of Personal Data under the Data Protection Laws of specific countries or jurisdictions. CareAR will provide notice of such changes to Customer, and the modified DPA will become effective, in accordance with the terms of the Agreement or as otherwise provided on CareAR's website if not specified in the Agreement.

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing)not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision.

controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three:Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four:Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU)2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, thoseterms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s)

of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subjectshall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the dataimporter under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available tothe data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter"sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a

third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the datasubject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into accountrelevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out withreasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

3 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/herhabitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation(EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU orMember State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance withits Article 3(2) and has appointed a representative pursuant to Article 27(1) ofRegulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1)

of Regulation (EU) 2016/679is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant toArticle 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competentsupervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access

by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards,[4]

(iii) or any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b),it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements maybe considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shallinclude information about the personal data requested, the requesting authority,the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to useits best efforts to obtain a waiver of the prohibition, with a view to communicating asmuch information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of thecontract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c)for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where itis unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the dataimporter shall seek interim measures

with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also makeit available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to thedata importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns theprocessing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletionof the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws

applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation(EU) 2016/679 that covers the transfer of personal data to which these Clauses apply;or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allowfor third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the country in which the data exporter is established or those of Ireland if Irish law is required as the governing law of these Clauses.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):
Customer that contracts for the services is the Data exporter/controller. Details required below are set forth in the Agreement between the Customer/Data Exporter and CareAR/Data Importer of which these Standard Contractual Clauses are a part. Where Customer contacts CareAR for any data related purpose governed by these Clauses, for example by sending an email to CareAR's privacy email (link below), then the Customer's contact details, so far as they are shown in any such communication, shall be deemed inserted below.

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these

uses: Signature and date:

Role (controller/processor):

Data importer(s):
CareAR is the data importer/processor. An additional method of contact for Data Importer may be found at https://carear.com/privacy-policy/.

Name: Nahum Cohen
Address: 5830 Granite Parkway #100, Suite 355, Plano, Texas 75024
Contact person's name, position and contact details: Nahum Cohen, VP of Technology & Cloud Operations, nahum.cohen@xerox.com

Activities relevant to the data transferred under these

Clauses: Details are set forth in the Agreement between

the Customer/Data Exporter and CareAR/Data Importer of

which these Standard Contractual Clauses are a part

Signature and date:

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Users of the Services

Categories of personal data transferred

First and Last Names
Email Addresses
Telephone numbers (at user's discretion)
User's Profile Photos (at user's discretion)
GPS coordinates (at user's discretion)
IP Address

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

None/Not Applicable.

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

Continuous basis as part of the Services.

Nature of the processing

Service Provider will process the personal data as necessary to perform the Services pursuant to the Agreement, the DPA, Terms of Service (available at https://carear.com/terms-of-Service/), as further specified in its Privacy Policy (available at https://carear.com/privacy-policy/), and as further instructed by Customer in its use of the Services.

Purpose(s) of the data transfer and further processing

To perform the contracted Services.

The period for which the personal data will be retained, or, if that is not possible, the criteriaused to determine that period

Upon termination of the contractual relationship between Customer and CareAR, personal data is retained for no more than sixty (60) days following final settlement of outstanding invoice(s) for services rendered.

……..

For transfers to (sub-) processors, also specify subject matter, nature and duration of theprocessing

Continuous basis as part of the Services and for the duration of the contract with the Customer/Data Exporter. See additional information on sub-processors at http://carear.com/gdpr-subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority/ies is that of the primary EU country of residence or incorporation of the Data Exporter.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

1. **Access Control to Processing Areas**.

Hosting providers are selected to ensure limited access to hosting areas. The providers must have the following controls:

- Equipment on which the personal data is processed is located in a physically protected site secured against physical access by unauthorized and/or uncontrolled individuals.
- Access authorizations are established for staff and third parties to the foregoing site. The list of entitled individuals is reviewed periodically to reflect fluctuations and changes in roles and responsibility.
- Access to the site is under control of specified management.
- Access to the site is established only to the identified group of people needed to support the required service level.
- Secured doors are in place to access the physical site.
- In addition, the site access is supervised and secured by an appropriate security system and/or security organization using a video control system.
- The physical site is only entered when work requiring access on site has to be done.

2. **Access Control to Data Processing Systems**.

Hosting providers are selected to ensure limited access to hosting systems. The providers must have the following controls:

- User Identification and user authentication methods to grant access to the processing system require individual authentication credentials such as user IDs or similar. Once assigned, they cannot be re-assigned to another person.
- Access control and authorizations are defined according to a 'need to have' principle. Users are uniquely identified and approved by business owners. User authentication credentials are deactivated when the user is no longer authorized from accessing the system, except for those accounts authorized solely for technical management.
- Use of privileged accounts is limited to specific functions and not used outside of the assigned function. Lists of system administrators are maintained and promptly updated on an ongoing basis.
- Internet and end user facing endpoints are protected to present unauthorized access to systems and malicious software including use of firewalls, antivirus/malware protection and detection.

3. **Access Control for Specific Areas Within Data Processing Systems; Data Loss Prevention**.

- Only authorized users are enabled to access personal data and access permissions/authorizations are set accordingly.
- Personal data cannot be read, copied, modified or removed without authorization.

4. **Protection During Transmission of Data**.

- Personal data is encrypted in transit.
- Network and network access protection technologies

- Data transfers are monitored for accuracy and completeness using networking protocols (TCP / TLS) with error correction features.

5. **Data Processing Controls**
   Functions supporting the processing of data and associated personnel are identified and documented.

6. **Availability Control**.
   Hosting providers are selected to ensure maximum availability. The providers must have the following controls:
   - The physical site where the data processing equipment is located is protected against general environmental hazard and unauthorized access.
   - It is protected with specific measures against power loss to ensure continuous service of the data centers even in the event of a power failure
   - It monitors and controls temperature and humidity at the site.
   - Availability of the network access to the site is enhanced thought WAN based redundancies and network access redundancies to the site.
   - Redundancies of the infrastructure components themselves (servers and storage arrays) are in place.
   - The redundancy measures are checked on a regular basis.
   - Functionalities are used on the database (DB) level to target for a minimum loss of transaction information in case of a technical failure. This is done by using DB features supporting minimal loss of transaction information were possible and meaningful.
   - In line with the service levels defined additional availability features on DB level (real application clustering) or at application level (application-based replication, load balancing) are in place.
   - To reduce unscheduled downtimes proactive infrastructure maintenance is done.

7. **General Controls**.
   Data importer will in addition apply the following procedures:
   - Policies in place regarding access to and protection of personal data are in place and employees are trained as to their obligations and the consequences of any violations of such obligations.
   - Regular checks of data protection measures are performed.
   - All personal data is encrypted at rest.
   - A data retention policy is in place to ensure that personal data is removed when no longer required and personal data collection is minimized where possible.
   - Technical and application related changes follow change management processes, supported where possible by multiple tiers where changes are applied first before being applied to the production environment
   - Changes to production environment are tracked and pre-approved.
   - After serious events a structured after-action review is executed to detect mitigation actions and potential proactive measures.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The controller has authorised the use of the following sub-processors:

The sub-processors listed at http://carear.com/gdpr-subprocessors and updated from time-to-time.

Subject to that, as at the date hereof and for information purposes, the sub-processors are shown below.

Name: Google GCP

Address: 1600 Amphitheatre Parkway.
Mountain View, CA 94043

Contact: Google DPO
https://support.google.com/cloud/contact/dpo

Description of processing: Hosting/User authentication

Name: Twillio/SendGrid

Address: 375 Beale St
Suite 300
San Francisco 94105

Contact: Office of the Data Protection Officer
privacy@twilio.com

Description of processing: SMS/email

Name: Agora.io

Address: 2804 Mission College Blvd.
Santa Clara, CA, USA 95054

Contact: Yaniv Elmadawi
VP, Solutions and Technology Services
yaniv@agora.io

Description of processing: Audio/Video transport

Name: Splunk

Address: 270 Brannan Street
San Francisco, CA 94107

Contact: dpacontracts@splunk.com

Description of processing: Logs aggregation

Name: Marketo

Address: 601 Townsend St
San Francisco, CA 94103
ATTN: Privacy, Legal

Contact: Data Protection Officer
privacyofficer@marketo.com

Description of processing: Signup forms

Name: Zuora

Address: 101 Redwood Shores Pkwy
Redwood City, CA 94065
(650) 779-4993

Contact: legal@zuora.com

Description of processing: subscription management

Name: Celonis

Address: 119 W 40th
16th Floor
New York, NY, 10018

Contact: Legal/CFO
cfo@celonis.com

Description of processing: Process analysis