Data Processing Addendum

1. Purpose

This Data Processing Addendum ("Addendum") supplements the terms and conditions in the Agreement as they relate to WellRight's Processing of Personal Data and compliance with Data Protection Law. The terms of this Addendum shall only apply to the extent WellRight receives Personal Data that is subject to Data Protection Law.

2. Definitions

Capitalized terms used but not defined have the meaning given in the Agreement. Other terms in this Addendum, which are not defined in the Agreement or this Addendum, shall have meanings consistent with any corresponding terms in Data Protection Law.

a) "Data Protection Law" means any applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which WellRight is subject, including, but not limited to, (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act and any binding regulations promulgated thereunder ("CCPA"), (b) the EU General Data Protection Regulation 2016/679 including the applicable implementing legislation of each Member State ("EU GDPR"), (c) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("UK GDPR" and together with the EU GDPR, the "GDPR"), (d) the Swiss Federal Act on Data Protection of 19 June 1992, (e) any other applicable law with respect to any Personal Data in respect of which WellRight is subject to, including the Colorado Privacy Act, the Virginia Consumer Data Protection Act, the Connecticut Data Protection Act, and the Utah Consumer Privacy Act , and (f) any other data protection law and any guidance or statutory codes of practice issued by any relevant Privacy Authority, in each case, as amended from time to time and any successor legislation to the same.

b) "Personal Data" means any information relating to, describes, is reasonably capable of being associated with, or could reasonably be linked to an identified or identifiable natural person ("Data Subject").

c) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, whether transmitted, stored, or otherwise Processed.

d) "Privacy Authority" shall mean any competent supervisory authority, attorney general, or other regulator with responsibility for privacy or data protection matters.

e) "Processing" means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. "Process" and "Processed" will have a corresponding meaning.

f) "Services" shall mean the services as described in the Agreement or any related order form or statement of work

g) "Standard Contractual Clauses" means the documentation set forth in Appendix A, as may be amended or replaced by the European Commission or other applicable Supervisory Authority.

h) "Supervisory Authority" shall mean: (a) in the context of the UK GDPR the UK Information Commissioner's Office; and (b) in the context of the EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

3. Processing Requirements

The parties agree that the details relating to the processing of Personal Data are set forth in Annex II.B of Appendix A. If required by Data Protection Law, WellRight, in its capacity as a data processor or sub-processor of Personal Data on Client's behalf, will:

a) Process Personal Data only on documented instructions from Client, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law to which WellRight is subject. In such case, WellRight will inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

b) Implement and maintain appropriate processes and any associated technical measures to assist Client in responding to data subject requests. To the extent WellRight receives a data subject request from an individual, WellRight shall direct that individual to Client. WellRight will reasonably assist Client to respond to data subject requests to the extent that Client is unable to access the relevant Personal Data in the use of the Services. For the avoidance of doubt, Client is responsible for responding to such requests and shall be responsible for any decisions it makes with regard to data subject requests;

c) Not reidentify, attempt to reidentify, or direct any other party to reidentify any data that has been deidentified, to the extent WellRight receives deidentified data from Client or the Processing under the Agreement allows for the deidentification of Personal Data.

d) permit Client to reasonably monitor WellRight's compliance with this Addendum, as required by Data Protection Law. WellRight will also make available to Client all information in WellRight's possession necessary to demonstrate that WellRight is in compliance with the obligation of Data Protection Law. Section 11 shall control with regard to the monitoring and demonstration of compliance required by this Section 3(d).

4. Security of Personal Data.

WellRight shall maintain, during the term of the Agreement, appropriate technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, as set forth in Annex II to Appendix A of this Addendum.

5. Confidentiality.

Without prejudice to any existing contractual arrangements between the parties, WellRight will treat all Personal Data as confidential and it will inform all its employees, agents and any approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. WellRight will ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

6. Subprocessors.

Client agrees that WellRight may engage third party sub-processors to process Personal Data in accordance with this Section.

a) Client hereby authorizes WellRight to appoint the sub-processors specified in Annex III to Appendix A of this Addendum.

b) WellRight shall provide Client prior notice of any additional or replacement sub-processors. After being notified, Client must notify WellRight within ten (10) business days of any reasonable objection it has to such sub-processors. Failure to notify WellRight within this time frame will constitute approval of such sub-processors.

c) In the event Client provides reasonable objection pursuant to Section 6(b), WellRight will use commercially reasonable efforts to make a change in Processing under the Agreement to avoid Processing of Personal Data by such sub-processor. If WellRight is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Client may terminate services provided under the Agreement in respect only to those services which cannot be provided by WellRight without the use of the objected-to sub-processor, by providing written notice to WellRight. Client shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated services.

d) In the event WellRight engages sub-processors under the Agreement, WellRight shall place the same or similar obligations in all material respects as those in this Addendum on such sub-processors or other obligations required by Data Protection Law. WellRight shall remain fully liable to Client for such sub-processors' performance of their obligations arising out of the Agreement.

7. Breach Notification

Unless otherwise prohibited by applicable law, WellRight will notify Client without undue delay upon becoming aware of a Personal Data Breach. Such notification shall include, to the extent such information is available (a) a detailed description of the Personal Data Breach, (b) the type of data that was the subject of the Personal Data Breach, and (c) the identity of each affected person (or, where not possible, the approximate number of Data Subjects and of Personal Data records concerned). In addition, WellRight shall communicate to Client (i) the name and contact details of WellRight's point of contact where more information can be obtained, (ii) a description of the likely consequences of the Personal Data Breach, (iii) a description of the measures taken or proposed to be taken by WellRight to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8. Client Obligations

Client is solely responsible for its use of the Services, including (a) obtaining any needed consents or authorizations for WellRight to Process Personal Data; (b) without limitation of WellRight's security obligations, making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (c) securing the account authentication credentials, systems and devices Client uses to access the Services; (d) securing Client's systems and devices that WellRight uses to provide the Services; and (e) backing up Personal Data. Client acknowledges and agrees to not transmit or send an individual's Personal Data to WellRight in the event an individual is no longer enrolled in the Services or if an individual has otherwise opted out of the Services or withdrawn his or her consent.

9. CCPA Requirements

a) WellRight shall not retain, use, or disclose Personal Data for any purpose other than to perform the services under the Agreement or otherwise as permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing such services.

b) WellRight shall not combine Personal Data with any other personal information, except as specifically instructed by Client in writing.

c) WellRight shall not use, retain, or disclose Personal Data outside of the direct business relationship between Client and WellRight, except as otherwise authorized or directed by Client.

d) WellRight shall not sell or share (as both terms are defined in the CCPA) rent, transfer, purport to transfer to a third-party Personal Data with for any purpose, except as specifically instructed by Client in writing.

e) WellRight shall notify Client in the event WellRight makes a determination that it can no longer meet its obligations under Data Protection Law.

f) WellRight certifies that it understands the requirements and restrictions in this Addendum with regard to its obligation under the CCPA.

10. Privacy Impact Assessments.

WellRight shall, promptly upon receipt of written request by Client (a) make available to Client such information as is reasonably necessary to demonstrate Client's compliance with Data Protection Law to the extent applicable to the Services, and (b) reasonably assist Client in carrying out any privacy impact assessment and any required prior consultations with Privacy Authorities, taking into account the nature of the Processing and the information available to WellRight. Unless such request follows a Personal Data Breach or is otherwise required by Data Protection Law, Client shall not make any such request more than once in any 12-month period.

11. Audit Rights.

If required by Data Protection Law, Client may audit WellRight's compliance with its obligations under this Addendum up to once per year and on such other occasions as may be required by Data Protection Law, including where mandated by Client's Privacy Authority. WellRight will contribute to such audits by providing Client or Client's Supervisory Authority with the information and assistance that WellRight considers appropriate in the circumstances and reasonably necessary to conduct the audit. To request an audit, Client must submit a proposed audit plan to WellRight at least two weeks in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. WellRight will review the proposed audit plan and provide Client with any concerns or questions (for example, any request for information that could compromise WellRight security, privacy, employment or other relevant policies). WellRight will work cooperatively with Client to agree on a final audit plan. Nothing in this Section 11 shall require WellRight to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor, Client agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and WellRight's safety, security or other relevant policies, and may not unreasonably interfere with WellRight business activities. Any audits are at Client's sole expense. Client shall reimburse WellRight for any time expended by WellRight and any third parties in connection with any audits or inspections under this Section 11 at WellRight's then-current professional services rates, which shall be made available to Client upon request. Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

12. Deletion of Personal Data

Upon Client's request, WellRight shall promptly delete or return all Personal Data to Client after the end of the provision of Services relating to Processing and delete existing copies unless applicable law requires WellRight to maintain Personal Data.

13. Legal Requests for Personal Data

Unless prohibited by applicable law, in the event that WellRight is required by law, court order, warrant, subpoena, or other legal judicial process ("**Legal Request**") to disclose any Personal Data to any person or entity other than Client, WellRight shall notify Client promptly and shall provide all reasonable assistance to Client, at Client's cost, to enable Client to respond or object to, or challenge, any such demands, requests, inquiries or complaints and to meet applicable statutory or regulatory deadlines. WellRight shall not disclose Personal Data pursuant to a Legal Request unless it is required to do so and has otherwise complied with the obligations in this Section.

14. International Transfers of Personal Data

Where Personal Data originating in the European Economic Area, United Kingdom, or Switzerland is Processed by WellRight outside the European Economic Area, United Kingdom, or Switzerland in a territory that has not been designated by the European Commission, United Kingdom or Switzerland as ensuring an adequate level of protection pursuant to Data Protection Law, WellRight and Client agree that any transfer or onward transfer shall be undertaken pursuant to Standard Contractual Clauses, as set forth on Appendix A. The Standard Contractual Clauses apply to Client or the affiliates of Client established within the European Economic Area, Switzerland or the United Kingdom that have signed Order Forms or are otherwise entitled to receive Services under the Agreement. For the purpose of the Standard Contractual Clauses, Client or the affiliates of Client shall be deemed "data exporters." For transfers from Switzerland only, the term "personal data" as used in the Standard Contractual Clauses, shall have the meaning give under the Swiss Data Protection Act, as amended or replaced from time to time.

15. Claims

Any claims brought under, or in connection with, this Addendum, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

16. Miscellaneous

The parties acknowledge and agree that, to the extent the Services contemplate the processing of Personal Data that is subject to Data Protection Law that require additional terms in this Addendum, the parties shall enter into an amendment to this Addendum that addresses such additional terms. In the event of any conflict between this Addendum and any data privacy provisions set out in the Agreement between the parties relating to the Services, the parties agree that the terms of this Addendum shall prevail. If and to the extent the Standard Contractual Clauses conflict with any provision of this Addendum, the Standard Contractual Clauses control and take precedence. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this Addendum, unless stated otherwise.

Effective Date: September 1st, 2023

APPENDIX A:
STANDARD CONTRACTUAL CLAUSES

The European Commission's Standard Contractual Clauses for Personal Data Transfers to Third Countries, (available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en) are hereby incorporated by reference as if set forth herein in full along with Annexes I, II, and III.

The United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the ICO in accordance with s119A of the Data Protection Act 2018 (the "UK Addendum") is also hereby incorporated by reference as if set forth herein in full.

Module 2 (Controller to Processor) shall be in effect for purposes of personal data transfers from the European Economic Area, the United Kingdom, and Switzerland between WellRight and Client. Client shall be the controller and data exporter under Module 2. WellRight shall be the processor and data importer under Module 2. The following Module 2 options and selections apply:

Clause 7 (Optional Docking Clause)	Not in effect
Clause 9a (Sub-Processor Option)	Option 2: General Written Authorization
Clause 9a (Sub-Processor Notice Period)	Thirty (30) days
Clause 11 (Optional Redress Language)	Not in effect
Clause 17 (Governing Law)	Ireland
Clause 18 (Choice of Forum and Jurisdiction)	Ireland

In addition, for the purposes of the UK Addendum: (a) Table 1 shall be completed with the information set out in Annex I.A; (b) for Table 2, the version of the Approved EU SCCs shall be Module 2 (Controller to Processor); (c) Table 3 shall be completed with the corresponding information in Annexes, I, II, and III; and (d) for Table 4, the option of "Importer" and "Exporter" shall be selected.

For Personal Data transfers from Switzerland, the following terms shall apply:

a. The term "Member State" as used in European Commission's Standard Contractual Clauses, including these Annexes, shall be interpreted as including Switzerland and data subjects in Switzerland.

b. Data subjects with their regular place of residence in Switzerland are allowed to bring a lawsuit in Switzerland against either the data exporter or the data importer in accordance with Clause 18(c) of the European Commission's Standard Contractual Clauses.

c. The European Commission's Standard Contractual Clauses will additionally protect data pertaining to Swiss legal entities until the revised Swiss Federal Act on Data Protection enters into force.

ANNEX I: DESCRIPTION OF PERSONAL DATA PROCESSING

A. LIST OF PARTIES

Data exporter(s):

The Client, as identified in the associated Agreement and Order Form, to which this Addendum is incorporated. Client's contact person's name and position for purposes of this Addendum is set forth on the relevant Order Form.

Activities relevant to the data transferred under these Clauses: To enable WellRight, Inc. to provide the Services, as outlined in the Agreement.

Client's execution of the Agreement and associated Order Forms constitutes Client's agreement to the Addendum and these Standard Contractual Clauses.

Data importer(s):

Name: WellRight, Inc.

Address: 175 W Jackson Blvd, Suite 1425 Chicago, IL 60604

Contact person's name, position and contact details: Philippe Lunardelli, Chief Financial Officer

Activities relevant to the data transferred under these Clauses: To provide the Services, as outlined in the Agreement.

Role (controller/processor): Processor

WellRights's execution of the Agreement and associated Order Forms constitutes its agreement to the Addendum and these Standard Contractual Clauses.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees and Employees' spouses and/or dependents

Categories of personal data transferred

First and last name ● Localization and demographic data ● Contact information (email, phone, physical address, mailing address) ● Data concerning health ● ID data ● IP address and device and browser data ● Data relating to usage of the Service

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into 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.

Health-related data.

See Annex 2 for safeguards

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

On a continuous basis during the term of the Agreement.

Nature of the processing

As described in the Agreement.

Purpose(s) of the data transfer and further processing

As described in the Agreement.

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

Until conclusion of the Services contemplated under the Agreement.

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

As described in the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies

Irish Data Protection Commission and Switzerland's Federal Data Protection and Information Commissioner*

*The Swiss Federal Data Protection and Information Commissioner is the supervisory authority only with respect to residents of Switzerland and their personal data.

ANNEX II: SECURITY POLICIES, PROCEDURES, CONTROLS

Description of the technical and organisational security measures implemented by WellRight:

Security Practices

WellRight has implemented corporate information security practices and standards that are designed to safeguard WellRight's corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by Processor's executive management and undergo a formal review on an annual basis.

Organizational Security

It is the responsibility of the individuals across the WellRight's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.

2. Security testing, design and implementation of security solutions to enable security controls adoption across the environment.

3. Security operations of implemented security solutions, the environment and assets, and manage incident response.

4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics, when necessary.

Physical and Environmental Security

WellRight uses a number of technological and operational approaches in its physical security program in regard to risk mitigation. WellRight's security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness's in business practice and expectations of data importer as a whole. WellRight balances its approach toward security by considering elements of control that include architecture, operations, and systems.

Communications and Operations Management

Incident response procedures exist for security incidents, which may include incident analysis, containment, response, remediation, reporting and the return to normal operations. To protect against malicious use of assets and malicious software, additional controls may be implemented based on risk. Such controls may include, but are not limited to, information security policies and standards, restricted access, designated development and test environments, virus detection on servers, desktop and notebooks;

virus email attachment scanning; system compliance scans, intrusion prevention monitoring and response, logging and alerting on key events, information handling procedures based on data type, ecommerce application and network security, and system and application vulnerability scanning.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges. Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

System Development and Maintenance

Vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

ANNEX III: AUTHORIZED SUB-PROCESSORS

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

Name	**Location of processing**	**Duration of processing**	**Description of processing (including a clear delimitation of responsibilities if multiple sub-processors are authorised and location where processing will take place)**
Amazon Web Services (AWS)	United States	As needed to provide services; no longer than term of Agreement.	Provides hosting services for the web infrastructure and databases
Validic	United States	As needed to provide services; no longer than term of Agreement.	Mobile health API connection to access user data gathered from clinical devices, and wearables devices
eHealthScreenings	United States	As needed to provide services; no longer than term of Agreement.	Provides biometric screening services
Tango Card	United States	As needed to provide services; no longer than term of Agreement.	E-Gift Card Rewards and Incentives management services
Marquee Health	United States	As needed to provide services; no longer than term of Agreement.	Provides employers with an outcomes-driven suite of health and wellness programs
Twilio	United States	As needed to provide services; no longer than term of Agreement.	Provides transactional SMS services