

Data Processing Agreement Addendum

THIS EUROPEAN DATA PROCESSING ADDENDUM ("European DPA") is entered into as of the _____ by and between: (1) ReaDI-Watch Ltd., an Irish corporation located at Suantraí, Curtlestown, Enniskerry, Co. Wicklow, Ireland ; and (2) _____ the entity or other person who is a counterparty to the Agreement (as defined below) into which the European DPA is incorporated and forms a part ("Customer"), together the "Parties" and each a "Party".

1. Definitions

Unless expressly stated otherwise, capitalised terms used in the European DPA have the meanings given below or, if not defined, have the meanings given in the Agreement. References to "including" mean "including, without limitation".

"Addendum Effective Date" means the effective date of the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Subject" means the identified or identifiable natural person to whom European Customer Data relates.

"Data Subject Request" means the request of a Data Subject to exercise rights under European Data Protection Laws in respect of European Customer Data in ReaDI-Watch's possession, custody or control.

"EEA" means the European Economic Area.

“European Customer Data” means Personal Data of Data Subjects in the EEA, United Kingdom, or Switzerland Processed by ReaDI-Watch or its Subprocessor(s) on behalf of Customer, or otherwise required to be Processed under and subject to European Data Protection Laws, to perform the Services under the Agreement.

“European Data Protection Laws” means the privacy, data protection and data security laws and regulations applicable to the Processing of European Customer Data in the EEA, United Kingdom and/or Switzerland under the Agreement, including the GDPR.

“FADP” means the Federal Act on Data Protection of 19 June 1992 and, as and when it enters into force on 1 January 2023, its revised version of 25 September 2020.

“FDPIC” means Swiss Federal Data Protection and Information Commissioner.

“GDPR” means, as and where applicable to Processing concerned (i) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”), (ii) the EU GDPR 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”), including, in each case (i) and (ii), any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to “Articles” and “Chapters” of, and other relevant defined terms in, the GDPR shall be construed accordingly.

“Personal Data” means information that relates to an identified or identifiable Data Subject.

“Personal Data Breach” means a breach of ReaDI-Watch’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, European Customer Data in ReaDI-Watch’s possession, custody or control.

“Process” and inflections thereof refer to any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

“Processor” means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

“Restricted Transfer” means any disclosure, grant of access, or other transfer of European Customer Data to any person located in (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission described in Chapter 45 of the GDPR (an “EU Restricted Transfer”), (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a “UK Restricted Transfer”), and (iii) in the context of Switzerland, a country or territory outside of Switzerland which does not benefit from an adequacy decision from the Swiss Government (a “Swiss Restricted Transfer”), in each case, which would be prohibited without a legal basis under the GDPR.

“SCCs” means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914, as populated in accordance with Part 1 of Annex 2.

“Services” means those services performed for Customer by ReaDI-Watch pursuant to the Agreement.

“Subprocessor” means any third party engaged directly or indirectly by or on behalf of ReaDI-Watch to Process European Customer Data.

“Supervisory Authority” means (i) in the context of the EEA and the EU GDPR, “supervisory authority” as defined in the EU GDPR; (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner’s Office; and (iii) in the context of Switzerland and the FADP, means the FDPIC.

“UK Transfer Addendum” means the template Addendum B.1.0 issued by the ICO under s119A of the Data Protection Act 2018, in force from 21 March 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the “UK Mandatory Clauses”).

2. Scope of this Data Processing Agreement

The Parties acknowledge and agree that the details of ReaDI-Watch's Processing of European Customer Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 to this DPA.

This DPA applies to ReaDI-Watch's Processing of European Customer Data. For the avoidance of doubt, the European DPA does not apply to ReaDI-Watch's Processing of Personal Data that does not constitute European Customer Data, and/or any other Processing of Personal Data with respect to Customer and Customer's users conducted by ReaDI-Watch as a Controller, including business relationship administration and system security.

3. Processing of Customer Personal Data

ReaDI-Watch shall not Process European Customer Data other than on Customer's instructions or as required by applicable laws. Customer instructs ReaDI-Watch to Process European Customer Data to provide the Services and as authorised by the Agreement. The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on ReaDI-Watch only pursuant to an amendment to the European DPA signed by both parties. Where ReaDI-Watch receives an instruction from Customer that, in its reasonable opinion, infringes European Data Protection Laws, ReaDI-Watch shall notify Customer.

The Parties acknowledge that ReaDI-Watch Processing of European Customer Data authorised by Customer's instructions stated in the European DPA are integral to the Services and the business relationship between the Parties. Access to Personal Data does not form part of the consideration exchanged between the Parties in respect of the Agreement or any other business dealings.

4. ReaDI-Watch Personnel

ReaDI-Watch shall ensure that all ReaDI-Watch employees or other personnel who Process European Customer Data are subject to contractual or appropriate statutory obligations of confidentiality with respect to such European Customer Data.

5. Security

ReaDI-Watch shall implement and maintain technical, organisational and physical measures designed to protect the confidentiality, integrity and availability of European Customer Data and

prevent Personal Data Breaches. Such measures shall include the measures described in Annex 3 of the European DPA (the “Security Measures”) and such other measures as are required by European Data Protection Laws. ReaDI-Watch may update the Security Measures from time to time, so long as the updated measures do not decrease in the aggregate the protection of Personal Data.

6. Restricted Transfers

General. The Parties acknowledge that Customer’s transmission of European Customer Data to ReaDI-Watch hereunder may involve a Restricted Transfer. The SCCs described in this section shall apply and have effect only if and to the extent permitted and required under the EU GDPR, UK GDPR, and/or FADP (if and as applicable) to establish a valid basis under the EU GDPR, UK GDPR, and/or the FADP in respect of a Restricted Transfer from Customer to ReaDI-Watch of European Customer Data.

EU Restricted Transfers. To the extent that any Processing of European Customer Data under the European DPA involves an EU Restricted Transfer from Customer to ReaDI-Watch, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be (a) populated in accordance with Part 1 of Annex 2; and (b) entered into by the Parties and incorporated by reference into the European DPA. UK Restricted Transfers. To the extent that any Processing of European Customer Data under the European DPA involves a UK Restricted Transfer from Customer to ReaDI-Watch, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be (a) varied to address the requirements of the UK GDPR in accordance with UK Transfer Addendum and populated in accordance with Part 2 of Annex 2; and (b) entered into by the Parties and incorporated by reference into the European DPA. The Parties agree that the manner of the presentation of the information included in the UK Transfer Addendum as set out in Part 2 of Annex 2 shall not operate or be construed so as to reduce the Appropriate Safeguards (as defined in the UK Mandatory Clauses).

Swiss Restricted Transfers. To the extent that any Processing of European Customer Data under the European DPA involves a Swiss Restricted Transfer from Customer to ReaDI-Watch, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be (a) varied to address the requirements of the FADP and populated in accordance with Part 3 of Annex 2; and (b) entered into by the Parties and incorporated by reference in the European DPA. Nothing in any applicable SCCs (as deemed amended pursuant to this Section)

should be interpreted or construed in such a way as would limit or exclude the rights of Data Subjects under Clause 18(c) of those SCCs (as deemed amended pursuant to this Section) to bring legal proceedings before the courts in Switzerland where Switzerland is that Data Subject's place of habitual residence.

Supplementary measures. In respect of any given Restricted Transfer, the Parties shall comply with their obligations under Annex 4 of the European DPA.

Provision of full-form SCCs. In respect of any given Restricted Transfer, on Customer's written request, ReaDI-Watch shall provide Customer with an executed version of the relevant set(s) of SCCs (amended and populated in accordance with Annex 2) in respect of the relevant Restricted Transfer.

7. Data Transfer Requests

ReaDI-Watch, taking into account the nature of the Processing of European Customer Data, shall provide Customer with such assistance by appropriate technical and organisational measures as Customer may reasonably request to assist Customer in fulfilling its obligations under European Data Protection Laws to respond to Data Subject Requests.

ReaDI-Watch shall promptly notify Customer if it receives a Data Subject Request and not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except as required by European Data Protection Laws.

Operational clarifications if and as the SCCs apply in accordance with Section 6:

When complying with its transparency obligations under Clause 8.3 of the SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, ReaDI-Watch's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

For the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

Where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Vendor to notify any third-party Controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

8. Personal Data Breaches

ReaDI-Watch shall notify Customer of a Personal Data Breach without undue delay after becoming aware of the occurrence thereof. ReaDI-Watch's notification of or response to a Personal Data Breach will not be construed as ReaDI-Watch's acknowledgement of any fault or liability with respect to the Personal Data Breach.

If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority or other governmental authority, any Data Subject(s), the public or others under European Data Protection Laws in a manner that directly or indirectly refers to or identifies ReaDI-Watch, where permitted by applicable laws, Customer agrees to notify ReaDI-Watch in advance and in good faith consult with ReaDI-Watch and consider any clarifications or corrections ReaDI-Watch may reasonably recommend or request to any such notification.

9. Sub-Processing

Customer generally authorises ReaDI-Watch to appoint Subprocessors in accordance with this Section 9. Without limitation to the foregoing, Customer authorises the engagement of the Subprocessors listed as of the effective date of the Agreement at the URL specified in this Section.

Information about Subprocessors, including their functions and locations, is available at: <https://readi-watch.com/legal> (as may be updated by ReaDI-Watch from time to time) or such other website address as ReaDI-Watch may provide to Customer from time to time (the "Subprocessor Site").

When engaging any Subprocessor, ReaDI-Watch will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in the European DPA with respect to European Customer Data to the extent applicable to the nature of the services provided by such Subprocessor. ReaDI-Watch shall be liable for all obligations

under the Agreement subcontracted to the Subprocessor or its actions and omissions related thereto.

When ReaDI-Watch engages any Subprocessor after the effective date of the Agreement, ReaDI-Watch will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the Subprocessor Site or by other written means at least thirty (30) days before such Subprocessor Processes European Customer Data. If Customer objects to such engagement in a written notice to ReaDI-Watch within ten (10) days after being notified of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and ReaDI-Watch will work together in good faith to consider a mutually acceptable resolution to such objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to ReaDI-Watch and pay ReaDI-Watch for all amounts due and owing under the Agreement as of the date of such termination.

Operational clarifications if and as the SCCs apply in accordance with Section 6:

The terms and conditions of this Section 9 apply in relation to ReaDI-Watch's appointment and use of Subprocessors under the SCCs.

Any approval by Customer of ReaDI-Watch's appointment of a Subprocessor that is given expressly or deemed given pursuant to Section 9 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Subprocessors if and as required under Clause 8.8 of the SCCs.

10. Compliance Assistance; Audits

ReaDI-Watch, taking into account the nature of the Processing and the information available to ReaDI-Watch, shall provide such information and assistance as Customer may reasonably request (insofar as such information is available to ReaDI-Watch and the sharing thereof does not compromise the security, confidentiality, integrity or availability of Personal Data Processed by ReaDI-Watch) to help Customer meet its obligations under European Data Protection Laws, including in relation to the security of European Customer Data, the reporting and investigation of Personal Data Breaches, the demonstration of Customer's compliance with such obligations, and the performance of any data protection assessments and consultations with Supervisory

Authorities or other government authorities regarding such assessments in relation to ReaDI-Watch's Processing of European Customer Data, including those required under Articles 35 and 36 of the GDPR.

ReaDI-Watch shall make available to Customer such information as Customer may reasonably request for ReaDI-Watch to demonstrate compliance with European Data Protection Laws and the European DPA in relation to ReaDI-Watch's Processing of European Customer Data.

Without limitation of the foregoing, Customer may conduct (in accordance with Section 10), at its sole cost and expense, and ReaDI-Watch will reasonably cooperate with, reasonable audits (including inspections, manual reviews, and automated scans and other technical and operational testing that Customer is entitled to perform under European Data Protection Laws), in each case, whereby Customer or a qualified and independent auditor appointed by Customer using an appropriate and accepted audit control standard or framework may audit ReaDI-Watch's technical and organisational measures in support of such compliance and the auditor's report is provided to Customer and ReaDI-Watch upon Customer's request.

Customer shall give ReaDI-Watch reasonable advance notice of any such audits. ReaDI-Watch need not cooperate with any audit (a) performed by any individual or entity who has not entered into a non-disclosure agreement with ReaDI-Watch on terms acceptable to ReaDI-Watch in respect of information obtained in relation to the audit; (c) outside normal business hours; or (d) on more than one (1) occasion in any calendar year during the term of the Agreement, except for any additional audits that Customer is required to perform under European Data Protection Laws. The audit must be conducted in accordance with ReaDI-Watch's safety, security or other relevant policies, must not impact the security, confidentiality, integrity or availability of any data Processed by ReaDI-Watch and must not unreasonably interfere with ReaDI-Watch's business activities. Customer shall not conduct any scans or technical or operational testing of ReaDI-Watch's applications, websites, Services, networks or systems without ReaDI-Watch's prior approval.

If the controls or measures to be assessed in the requested audit are assessed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified and independent third-party auditor pursuant to a recognized industry standard audit framework within twelve (12) months of Customer's audit request ("Audit Report") and ReaDI-Watch has confirmed in writing that there have been no known material changes to the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an

audit under Section 10. ReaDI-Watch shall provide copies of any such Audit Reports to Customer upon request.

Such Audit Reports and any other information obtained by Customer in connection with an audit under this Section 10 shall constitute confidential information of ReaDI-Watch, which Customer shall use only for the purposes of confirming compliance with the requirements of the European DPA or meeting Customer's obligations under European Data Protection Laws. Nothing in this Section 10 shall be construed to obligate ReaDI-Watch to breach any duty of confidentiality.

Operational clarifications if and as the SCCs apply in accordance with Section 6:

The audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in this Section 10.

11. Return and Deletion

Upon expiration or earlier termination of the Agreement, ReaDI-Watch shall return and/or delete all European Customer Data in ReaDI-Watch's care, custody or control in accordance Customer's instructions as to the post-termination return and deletion of Customer Data expressed in the Agreement, or subject to Section 12, Customer's further instructions.

Notwithstanding the foregoing, ReaDI-Watch may retain European Customer Data where required by applicable laws, provided that ReaDI-Watch shall (a) maintain the confidentiality of all such European Customer Data and (b) Process the European Customer Data only as necessary for the purpose(s) and duration specified in the applicable law requiring such retention.

Operational clarifications if and as the SCCs apply in accordance with Section 6:

Certification of deletion of European Customer Data as described in Clauses 8.5 and 16(d) of the SCCs, shall be provided only upon Customer's written request.

12. Customer Responsibilities

Customer agrees that, without limiting ReaDI-Watch's obligations under Section 5, Customer is solely responsible for its use of the Services, including (a) making appropriate use of the

Services to maintain a level of security appropriate to the risk in respect of the Customer Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that ReaDI-Watch uses to provide the Services; and (d) backing up Customer Data.

Customer shall ensure that there is, throughout the term of the Agreement, a valid legal basis for ReaDI-Watch's Processing of European Customer Data in accordance with the Agreement for the purposes of European Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR where applicable). Customer shall ensure (and is solely responsible for ensuring) that all required notices have been given to, and all consents and permissions have been obtained from, Data Subjects and others as are required, including under European Data Protection laws, for ReaDI-Watch to Process European Customer Data as contemplated by the Agreement.

Customer agrees that the Service, the Security Measures, and ReaDI-Watch's commitments under the European DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under European Data Protection Laws, and provide a level of security appropriate to the risk in respect of the European Customer Data.

Customer shall ensure that European Customer Data made available to ReaDI-Watch for Processing does not contain any (a) Social Security numbers or other government-issued identification numbers; (b) biometric information; (c) passwords to any online accounts; (d) credentials to any financial accounts; (e) tax return data; (f) any payment card information subject to the Payment Card Industry Data Security Standard; (g) Personal Data of children under 16 years of age; (h) data relating to criminal convictions and offences or related security measures; or (i) information that constitutes special categories of personal data (as defined in the GDPR) or information of a similarly sensitive character regulated by European Data Protection Laws.

Except to the extent prohibited by applicable law, Customer shall compensate ReaDI-Watch at ReaDI-Watch's then-current professional services rates for, and reimburse any costs reasonably incurred by ReaDI-Watch in the course of providing, cooperation, information or assistance requested by Customer pursuant to Sections 6, 10 and 11 of the European DPA beyond ReaDI-Watch's provision of any self-service tools as part of the Services that Customer can use to obtain the requested cooperation, information or assistance.

13. Liability

Nothing in the Agreement (including the European DPA) shall limit either party's liability to Data Subjects under the third-party beneficiary provisions of the SCCs.

14. Precedence

In the event of any conflict or inconsistency between (a) the European DPA and the Agreement, the European DPA shall prevail; (b) the European DPA and any other agreement made between the parties as relates to Personal Data, the European DPA shall prevail; or (b) any SCCs entered into pursuant to Section 6 and the European DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply. Annex 1

Annex 1 - Data Processing Details CUSTOMER / 'DATA EXPORTER' DETAILS

Name: _____

Customer Activities: The use and receipt of Services under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of its ongoing business operations

Role:

(a) Controller – in respect of any Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and

(b) Processor – in respect of any Processing of Customer Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including its Affiliates if and where applicable).

ReaDI-Watch / 'DATA IMPORTER' DETAILS

Name: ReaDI-Watch Ltd.

Contact details for data protection: dbyrne@readi-watch.com

Customer Activities: Research, Development, and Innovation Management Software

Role: Processor

DETAILS OF PROCESSING

Categories of Data Subjects: Any individuals whose Personal Data is comprised within data submitted to the Services by or on behalf of Customer under the Agreement, which will be as determined by Customer in its sole discretion through its use of the Services – but may include Customer's and its Affiliates':

1. "Staff", namely:
 - a. employees and non-employee workers;
 - b. students, interns, apprentices and volunteers;
 - c. directors and officers;
 - d. advisers, consultants, independent contractors, agents and autonomous, temporary or casual workers.
2. Customers, clients, (sub-)licensees, users and end-users, website visitors and marketing prospects.
3. Suppliers, service providers, consultants, advisers and other providers of goods or services.
4. Distributors, resellers, sales agents, introducers, sales representatives, collaborators, joint-venturers and other commercial partners.
5. Shareholders, partners, members and supporters.
6. Advisers, consultants and other professionals and experts.

Where any of the above is a business or organisation, it includes their Staff.

Each category includes current, past and prospective Data Subjects.

Categories of Personal Data: Any Personal Data comprised within data submitted to the Services by or on behalf of Customer under the Agreement, which will be as determined by Customer in its sole discretion through its use of the Services – but may include:

1. Personal details, including any information that identifies the Data Subject and their personal characteristics, including: name, address, contact details (including email

address, telephone details and other contact information), age, date of birth, sex, and physical description.

2. Technological details, such as internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.

Sensitive Categories of Data, and associated additional restrictions/safeguards:

Categories of sensitive data: None – as noted in Section 12 of the DPA, Customer agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the SCCs), must not be submitted to the Services.

Additional safeguards for sensitive data: N/A

Frequency of transfer: Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.

Nature of the Processing: Processing operations required in order to provide the Services in accordance with the Agreement.

Purpose of the Processing: European Customer Data will be Processed: (i) as necessary to provide the Services as initiated by Customer in its use thereof, and (ii) to comply with any other reasonable instructions provided by Customer in accordance with the terms of this DPA.

Duration of Processing / Retention Period: For the period determined in accordance with the Agreement and DPA.

Transfers to (sub)processors: Transfers to Subprocessors are as, and for the purposes, described from time to time in the Subprocessor Site (as may be updated from time to time in accordance with Section 9 of the DPA).

Annex 2 – Population of SCCs

In the context of any EU Restricted Transfer, the SCCs populated in accordance with Part 1 of this Annex 2 are incorporated by reference into and form an effective part of the European DPA (if and where applicable in accordance with Section 6 of the European DPA).

In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Annex 2 are incorporated by reference into and form an effective part of the European DPA (if and where applicable in accordance with Section 6 of the European DPA).

In the context of any Swiss Restricted Transfer, the SCCs as varied and populated by Part 3 of this Annex 2 are incorporated by reference into and form an effective part of the European DPA (if and where applicable in accordance with Section 6 of the European DPA).

PART 1: POPULATION OF SCCs

1. Signature of the SCCs; Modules

Where applicable in accordance with Section 6 of the European DPA, (a) each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs; and (b) those SCCs are entered into by and between the Parties with effect from (i) the effective date of the Agreement; or (ii) the date of the first Restricted Transfer to which they apply in accordance with Section 6 of the European DPA, whichever is the later.

The following Modules of the SCCs apply in the manner set out below (having regard to the role(s) of Customer set out in Annex 1 to the European DPA):

- a. Module Two of the SCCs applies to any EU Restricted Transfer and/or Swiss Restricted Transfer involving Processing of European Customer Data in respect of which Customer is a Controller in its own right.
- b. Module Three of the SCCs applies to any EU Restricted Transfer and/or Swiss Restricted Transfer involving Processing of European Customer Data in respect of which Customer is a Processor acting on behalf of any other person (including its Affiliates if and where applicable).

2. Population of the Body of the SCCs

For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

- A. In Clause 7: the 'Docking Clause' is not used.
- B. In Clause 9: 'OPTION 2: GENERAL WRITTEN AUTHORIZATION' applies, and the minimum time period for advance notice of the addition or replacement of Subprocessors shall be the advance notice period set out in Section 9 of European DPA, and the list of Subprocessors already authorised by the data exporter shall be the list on the Subprocessor Site as of the effective date of the Agreement;
- C. In Clause 11: the optional language is not used.
- D. In Clause 13: all square brackets are removed and all text therein is retained
- E. In Clause 17: 'OPTION 1' applies, and the Parties agree that the SCCs shall governed by the law of Ireland in relation to any EU Restricted Transfer; and
- F. In Clause 18(b): the Parties agree that any dispute arising from the SCCs in relation to any EU Restricted Transfer shall be resolved by the courts of Ireland.

In this Section, references to "Clauses" are references to the Clauses of the SCCs.

3. Population of the Annexes to the Appendix to the SCCs

Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 to the European DPA, with Customer being 'data exporter' and ReaDI-Watch being 'data importer'.

Part C of Annex I to the Appendix to the SCCs is populated as follows:

- A. Where Customer is established in an EU Member State, the competent supervisory authority shall be the supervisory authority of that EU Member State in which Customer is established.
- B. Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which Customer's EU representative relevant to the processing hereunder is based (from time-to-time).

- C. Where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies, but Customer has not appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to ReaDI-Watch's contact point for data protection identified in Annex 1 to the European DPA, which must be an EU Member State 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.

Annex II to the Appendix to the SCCs is populated as below:

- A. General: Please refer to Section 5 of the European DPA and the Security Measures described therein and the supplementary measures described in Annex 4 of the European DPA. In the event that Customer receives a Data Subject Request under the EU GDPR and requires assistance from ReaDI-Watch, Customer should email ReaDI-Watch's contact point for data protection identified in Annex 1 to the European DPA.
- B. Subprocessors: When ReaDI-Watch engages a Subprocessor under these Clauses, ReaDI-Watch shall enter into a binding contractual arrangement with such Subprocessor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the European DPA – including in respect of (a) applicable information security measures; (b) notification of Personal Data Breaches to ReaDI-Watch; (c) return or deletion of European Customer Data as and where required; and (d) engagement of further Subprocessors.

Annex III to the Appendix to the SCCs is populated as described in Section 9 of the European DPA.

PART 2: UK RESTRICTED TRANSFERS

1. UK Transfer Addendum

Where applicable in accordance with Section 6 of the European DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below –

- A. Part 1 to the UK Transfer Addendum. As permitted by Section 17 of the UK Transfer Addendum, the Parties agree:
- a. Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 to the European DPA and the foregoing provisions of this Annex 2 (subject to the variations effected by the UK Mandatory Clauses described in (b) below); and
 - b. Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.
 - c. Part 2 to the UK Transfer Addendum. The Parties agreed to be bound by the UK Mandatory Clauses of the UK Transfer Addendum.

In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the European DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in Section 1 this Part 2.

PART 3: SWISS RESTRICTED TRANSFERS

1. Variations for Swiss Restricted Transfers

Where applicable in accordance with Section 6 of the European DPA, the SCCs also apply in the context of Swiss Restricted Transfers with the following terms deemed to have the following substituted meanings:

1. "GDPR" means the FADP;
2. "European Union", "Union" and "Member State(s)" each mean Switzerland; and
3. "supervisory authority" means the FDPIC.

In relation to any Swiss Restricted Transfer to which they apply, where the context permits and requires, any reference in the European DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in Section 1 of this Part 3.

Annex 3 – Security Measures

ReaDI-Watch agrees to implement and maintain the security measures detailed under the section "**How We Protect This Data**" of the Data Management Policy found at <https://readi-watch.com/legal>.

Annex 4 – Supplementary Measures

ReaDI-Watch has implemented the following supplementary measures in respect of European Customer Data subject to a Restricted Transfer (“Transferred Personal Data”):

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, ReaDI-Watch implements and maintains appropriate technical and organisational measures to (i) ensure the security and confidentiality of Transferred Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Transferred Personal Data; and (iii) protect against any Personal Data Breach, including, without limitation, by implementing and maintaining the Security Measures.

2. ReaDI-Watch represents and warrants that (i) it has not purposefully created backdoors or similar programming that could be used to access its systems or Transferred Personal Data, (ii) it has not purposefully created or changed its business processes in a manner that facilitates access to its systems or to Transferred Personal Data by government authorities and shall not voluntarily cooperate with government authorities in relation to the same, and (iii) no applicable law or government policy to which ReaDI-Watch is subject requires ReaDI-Watch to create or maintain backdoors or to facilitate access to Transferred Personal Data or systems or for ReaDI-Watch to be in possession of any corresponding encryption keys. ReaDI-Watch agrees and warrants that it has no reason to believe that the legislation applicable to it, or its Subprocessors, including in any country to which Transferred Personal Data is transferred either by itself or through a Subprocessor, prevents it from fulfilling the instructions received from Customer and its obligations under the European DPA 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 European DPA, ReaDI-Watch will promptly notify the change to Customer as soon as ReaDI-Watch is aware, in which case Customer is entitled to suspend the transfer of Transferred Personal Data or terminate the Agreement.

3. In case ReaDI-Watch receives a disclosure order, ReaDI-Watch will (i) assess the legality of the request under applicable law; (ii) exhaust all available remedies to challenge the request where there are legal grounds to do so; (iii) document such legal assessment and challenges to the request; (iv) upon request, make such documentation available to Customer and the competent Supervisory Authority. ReaDI-Watch will reasonably cooperate with Customer in relation to such request and provide Customer with prompt updates at regular intervals with

regards to any additional information related to the request. Customer will have the right to defend such action in lieu of and/or on behalf of ReaDI-Watch. Customer may, if it so chooses, seek a protective order. ReaDI-Watch will reasonably cooperate with Customer in such defence.

4. (i) ReaDI-Watch will notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Transferred Personal Data. Such notification shall include details regarding the Data Subject concerned, Transferred Personal Data requested, the requesting authority, the legal basis for the request, and any responses provided. (ii) Where ReaDI-Watch is prohibited from satisfying clause (i) under applicable law, ReaDI-Watch will use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. ReaDI-Watch agrees to document its best efforts in order to be able to demonstrate them on request of Customer. (iii) Where ReaDI-Watch becomes aware of any direct access by government authorities to Transferred Personal Data (including the reasonable suspicion thereof), ReaDI-Watch will promptly notify Customer with all information available to ReaDI-Watch, unless otherwise prohibited by applicable law. (iv) For the purposes of Clause 15.1(a) of the SCCs, ReaDI-Watch will notify Customer only and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

5. ReaDI-Watch will (i) treat Transferred Personal Data as confidential information subject to the Agreement's confidentiality terms, and shall not disclose Transferred Personal Data to any third parties other than in accordance with the Agreement; (ii) grant access to Transferred Personal Data only to employees, agents, representatives, and subcontractors who need such access for the scope of the performance of the Services; (iv) ensure that persons authorized to Process the Transferred Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality that survive termination of the personnel engagement, and are fully qualified and trained regarding the handling of Transferred Personal Data.

6. ReaDI-Watch will document and record the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved. These records will be made available to Customer, who shall in turn provide them to the Data Subject(s) concerned.

7. ReaDI-Watch will publish transparency reports annually or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by applicable law. It can be assumed that the lack of this publication indicates that no such requests for access to data have been made.