IXICARE BV
Warande 13B, 9270 Laarne
BE 0657.749.278

Annex 3: DPA (Data Processing Agreement)

— Article 1. Subject and definitions

1.1. In the context of the Agreement, ixicare shall process personal data on behalf of and in accordance with the Partner's instructions. ixicare acts as the processor ("**Processor**") and the Partner acts as the data controller ("**Data controller**").

1.2. The purpose of this Processor agreement is to lay down the provisions governing the processing of personal data between the Data controller and the Processor in the context of their entire contractual relationship, regardless of whether this is documented in writing or agreed orally.

1.3. All terms used in this Processor agreement that have been defined in the General Data Protection Regulation (Regulation (EU) 2016/679, hereinafter referred to as "**GDPR**") shall have the same meaning as in the GDPR, unless expressly stated otherwise in this Processor agreement.

— Article 2. Instructions of the Data controller

2.1. The Processor shall process the Personal data solely on behalf of and in accordance with the Data controller's written instructions, specifically as set out in this article. In processing the Personal data, the Processor undertakes to respect the subject matter, duration, nature and purpose of the processing, as well as the categories of Personal data and data subjects to be processed.

2.2. The Parties shall process the Personal data in accordance with the applicable regulations on the processing and protection of personal data, including the GDPR.

2.3. The Data controller guarantees that it shall only issue instructions, guidelines or communications to the Processor that comply with the applicable regulations on the processing and protection of personal data, including the GDPR.

2.4. The Processor shall inform the Data controller if it believes that any instruction given by the Data controller violates the applicable regulations on the processing and protection of personal data.

2.5. **Purposes and Subject**. The processing activities carried out by the Processor on the instructions of the Data controller are aimed at providing the Services by the Processor in pursuance of the Agreement, including the necessary transmission, access and storage of personal data relating to the data subjects specified in this article. The Services comprise, but are not limited to, the provision of an emergency and alert system with both indoor and outdoor tracking capabilities.

2.6. **Categories of Personal data.** The Personal data processed by the Processor on the Data controller's instructions comprise:

- Identification data (such as surname, first name, phone number, password, IP address).
- Personal characteristics (such as sex, date of birth).
- Location data (such as positioning via beacons and GPS).
- Data relating to incidents and alarms (such as automatic and manual alarm signals).
- Data relating to physical and mental health.
- Log data relating to the use of the ixicare system.

2.7. **Data subjects.** The Data subjects of the aforementioned data are persons who wear the ixicare device or use the Services (directly or indirectly), and comprise:

- Residents or users under the care of the Data controller
- Healthcare providers, staff members and/or other service providers acting on behalf of the Data controller
- Family and visitors of the residents or users

2.8. **Term.** Personal data shall be processed by the Processor for as long as the Services are provided in pursuance of the Agreement, unless otherwise specified in this Processor agreement.

2.9. The Processor is permitted to further process the Personal data for the purpose of improving the Services, in particular through internal (big) data analysis and statistical or scientific studies.

— Article 3. Non-disclosure

3.1. The Processor shall treat the Personal data and the existence of the processing on behalf of the Data controller with the greatest confidentiality.

3.2. The Processor shall not disclose or make the Personal data accessible to third parties, subject to prior written consent, legal obligation or order from a competent authority.

3.3. If the Processor contracts third parties, it shall guarantee that they are contractually bound by at least the same obligations. The Processor shall restrict access to the Personal data to employees who strictly require it. The Processor guarantees that all individuals authorised by or on behalf of the Processor to process Personal data are bound by a duty of non-disclosure. The Processor shall ensure that such individuals only access Personal data to the extent necessary for the performance of their duties in the context of this Processor agreement and that they have received instructions regarding the applicable data protection and non-disclosure obligations.

— Article 4. Assistance to the Data controller

4.1. **Observance of the law and obligation to provide information.** The Parties shall assist each other in fulfilling their obligations in pursuance of the GDPR, taking into account the nature of the processing and the information available to them. The Processor shall provide the Data controller with all information necessary to demonstrate compliance with its obligations in pursuance of the

GDPR. The Processor shall report any complaints, queries or concerns raised by data subjects without undue delay and shall act only in accordance with instructions.

4.2. **Personal data breach.** In the event of a Personal data breach relating to processing activities in pursuance of the Agreement, the Processor shall support the Data controller in accordance with Articles 32–36 of the GDPR, and specifically the following:

- the Processor shall notify the Data controller of the breach without delay and no later than 48 hours.

- notification shall include the nature of the breach, categories of data subjects and data, numbers, contact details, consequences and measures.

- the Processor shall assist, where possible, with notifications to supervisory authorities and/or data subjects.

- the Parties shall cooperate in good faith to limit any adverse effects resulting from a Personal data breach.

It is the exclusive responsibility of the Data controller to assess the severity of the breach and to notify the supervisory authority and/or the data subjects, as appropriate, of a personal data breach.

4.3. **Data Protection Impact Assessment (DPIA).** If a DPIA is required, it shall be carried out by the Data controller. The Processor shall provide all necessary cooperation. The Processor is entitled to charge reasonable fees for such assistance, which must be proportionate to the services provided.

4.4. **Rights of data subjects.** Taking into account the nature of the processing, the Processor shall assist the Data controller by means of appropriate technical and organisational measures, in so far as possible, in fulfilling its duty to respond to requests concerning the exercise of the Data subject's rights under Chapter III of the GDPR.

Article 5. Obligations of the Parties

5.1. The Parties shall treat each other's reasonable requests relating to the processing of Personal data under this Processor Agreement and/or the Agreement either immediately or within a reasonable term.

5.2 The Parties shall agree on appropriate communication channels to ensure that instructions, guidelines and other communications relating to Personal data processed by the Processor on behalf of the Data controller are properly received by the Parties. The Parties shall inform each other of the identity of the person who is the single point of contact

5.3. The Parties shall cooperate in good faith to limit any adverse effects resulting from incidents that affect the Personal data processed by the Processor and/or its sub-processors in pursuance of this Processor agreement on the Controller's instructions.

Article 6. The use of sub-processors

6.1. The Data controller grants the Processor general permission to contract sub-processors in the performance of the processing activities. A list of sub-processors already approved at the time of signing this Processor agreement is available at: https://ixicare.com/subprocessors and may be requested by the Data controller at any time.

6.2. The Processor shall inform the Data controller in advance of any intended changes concerning the addition or replacement of sub-processors. The Data controller has the right to object to such changes within 30 days of receiving such notification, provided the objection is based on reasonable grounds relating to data protection. If the Data controller raises an objection and the parties cannot reach a resolution, the Data controller shall have the right to terminate the Agreement, insofar as it relates to the relevant processing, without incurring any costs.

6.3. The Processor shall ensure, to the extent that is deemed reasonably possible, that sub-processors are bound by the same data protection obligations that are at least equivalent to the obligations set out in this Processor agreement, so as to ensure an appropriate level of protection for the Personal data.

6.4. The Processor shall remain fully liable vis-à-vis the Data controller for the observance of the sub-processor's obligations.

Article 7. Security measures

7.1. The Processor shall take appropriate technical and organisational measures to secure the Personal data. An overview of technical and organisational measures is available via the website: https://ixicare.com/TOM. More information may be provided by the Processor upon first request.

7.2. In assessing appropriate technical and organisational security measures, the following shall be taken into account: (i) the state of the art, (ii) the costs of the implementation of these measures, (iii) the nature, scope, context and purposes of the processing, (iv) the varying likelihood and severity of risks to the rights and freedoms of persons.

7.3. The technical and organisational measures are aimed at ensuring a level of security aligned to the risk, taking into account privacy risks, particularly those resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, transmitted, stored or otherwise processed data.

7.4. Where appropriate, the technical and organisational measures shall include, among others:

a) the pseudonymisation and encryption of personal data;

b) the ability to permanently safeguard the confidentiality, integrity, availability and resilience of the processing systems and services;

c) the ability to restore the availability of, and access to, personal data on time in case of a physical or technical incident;

d) a procedure for periodically testing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure the security of the processing.

7.5. These measures shall be updated in accordance with the state of the art and in response to any incidents.

Article 8. Audit and inspection

8.1. The Data controller shall have the right to conduct audits or inspections at the Processor, solely to the extent necessary to verify compliance with this Processor agreement and the applicable provisions of the GDPR.

8.2. Audits and inspections shall only take place following prior written notice of at least thirty (30) calendar days and no more than once per calendar year, unless (i) required by a Supervisory Authority, or (ii) there is a reasonable suspicion of a serious breach of this Processor agreement or the GDPR by the Processor.

8.3. Audits shall be conducted by an independent, expert third party bound by confidentiality, who has been approved in writing by the Processor (such approval shall not be unreasonably withheld).

8.4. Audits and inspections shall be conducted during regular business hours and in a manner that minimises disruption to the Processor's operations. All audit costs shall be fully borne by the Data controller, unless the audit reveals an essential failure by the Processor to comply with its obligations on the grounds of this Processor agreement or the GDPR.

Article 9. Transfer of personal data outside the EEA

9.1. A transfer to a country or international organisation outside the European Economic Area (EEA) is permitted provided that (1) the transfer is carried out based on documented instructions from the Data controller or is required on the grounds of a legal obligation enforceable under EU or Belgian law, (2) the country or the enterprise(s) to which the data are transferred ensure an adequate level of protection for personal data and/or (3) the transfer is carried out in accordance with the European Commission's standard contract clauses.

9.2. The Processor shall obtain the Data controller's prior written consent for any intended transfer of personal data outside the European Economic Area and shall ensure that such transfers comply with the conditions set out in this Article 9.

9.3. When the Processor relies on standard contractual clauses ("SCCs") or other appropriate safeguards, it shall provide evidence of such safeguards to the data manager upon request. In the event of transfers to a country not covered by an adequacy decision, the Processor shall provide evidence of the risk assessment conducted regarding the recipient country's legal framework and of the risk mitigation measures taken to ensure an adequate level of protection for the transferred personal data.

Article 10. Retention time, return and removal of personal data

10.1. The Processor shall retain the Personal data only for as long as necessary for the purposes, unless a statutory retention obligation applies.

10.2. Upon completion or termination of the processing activities, the Processor shall, at the Data controller's discretion, delete all Personal data or return them to the Data controller and delete all existing copies and confirm that this has been done, unless retention of the Personal data is required by law.