This data processing agreement is applicable to all processing of personal data to be undertaken by SYN LTD, registered with the Companies House with number 09243303, (hereinafter: Processor) for the benefit of another party to whom it provides services (hereinafter: Controller) on the basis of the agreement concluded between these parties (hereinafter: the Agreement).

Article 1. Purposes of processing

1. Processor hereby agrees under the terms of this Data Processing Agreement to process personal data commissioned by the Controller. Processing shall be done for the sole purpose of storing data in the 'cloud' for the benefit of Controller, and associated online services, and all purposes compatible therewith or as determined in accordance with the Controller.
2. The personal data to be processed by Processor for the purposes set out in the previous clause and the categories of those parties involved are set out in Appendix 1 to this Data Processing Agreement. Processor shall not process personal data for any other purpose than has been determined by Controller. Controller shall inform Processor of any processing purposes to the extent for as far as these are not already mentioned in this Data Processing Agreement.
3. The commissioned personal data processed on behalf of Controller shall remain the property of Controller and/or those parties involved.

Article 2. Processor obligations

1. Regarding the processing operations referred to in Article 1, Processor shall comply with all applicable legislation and regulations , including at least all data protection legislation such as the General Data Protection Regulation (GDPR).
2. Upon first request Processor shall inform Controller about any measures taken to comply with its obligations under this Data Processing Agreement.
3. All obligations for Processor under this Data Processing Agreement shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in its widest sense.
4. Processor shall inform Controller without delay if, in its opinion, an instruction of Controller would violate with the legislation referred to in Article 1.
5. Processor shall provide assistance, within its power, to Controller for the purpose of any data protection impact assessments to be made by Controller.
6. Processor shall, in accordance with Article 30 GDPR, keep a register of all categories of processing activities which it carries out on behalf of the Controller under this Data Processing Agreement. At Controller's request, Processor shall provide Controller access to this register.

Article 3. Transfer of personal data

1. Processor may process the personal data in any country within the European Union.
2. Transfer to countries outside the European Union is not permitted.

Article 4. Allocation of responsibilities

1. The Processor wil provide ICT resources for the purpose of processing that may be used by the Controller for the above mentioned purposes. Personnel of the Processor will only perform processing of data on the basis of separate agreement.
2. Processor is solely responsible for the processing of personal data under this Data Processing Agreement in accordance with the instructions of Controller and under the explicit supervision of Controller. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor explicitly does not accept any responsibility.
3. Controller represents and warrants that the content, usage and instructions to process the personal data as meant in this Data Processing Agreement are lawful and do not violate any right of any third party.

Article 5. Involvement of sub-processors

1. Processor shall involve third parties in the processing under this Data Processing Agreement on the condition that such parties are reported in advance to the Controller; Controller may object to a specific third party if its involvement would reasonably be unacceptable to Controller.
2. In any event, Processor shall ensure that any third parties are bound in writing to at least the same obligations as agreed between Controller and Processor.
3. Processor represents and warrants that these third parties shall comply to the obligations under this Data Processing Agreement and is liable for any damages caused by violations of these third parties as if it committed the violation itself.

Article 6. Security

1. Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).
2. Processor shall implement at least the following specific security measures:
    - A secure internal network
    - Physical access control measures
    - Organizational measures for access control
    - Logical access control, using : strong passwords, personal access cards
    - Automatic logging of all operations concerning personal data
    - Random checks for compliance with its policies
    - Purpose-bound access controls
    - Secure Socket Layer (SSL) technology for securing network communication
    - Checks on granted authorizations
3. Processor does not warrant that the security is effective under all circumstances. If any security measure explicitly agreed in this Data Processing Agreement is missing, then Processor shall use best efforts to ensure a level of security appropriate to the risk taking into account the state-of the art of current technology, the sensitivity of

the personal data and that the cost of implementation of this security is not unreasonable.

4. Controller shall only provide personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for the parties' compliance with these security measures.
5. Processor operates in accordance with
    - ISO 27001
    - NEN 7510, Information security in the health care industry
    - PCI Security Standards
    - ISAE 3402

    These standards are considered to meet the demands on information security given the current state of art.

Article 7. Notification and communication of data breaches

1. Controller is responsible at all times for notification of any security breaches and/or personal data breaches (defined as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) to the competent supervisory authority, and for communication of the same to parties involved. In order to enable Controller to comply with this legal requirement, Processor shall notify Controller within a reasonable period after becoming aware of an actual or threatened security or personal data breach.
2. A notification under the previous clause shall be made at all times, but only for actual breaches.
3. The notification shall at least include the fact that a breach has occurred. In addition, the notification shall:
    - describe the nature of the personal data breach including, where possible, the categories and approximate number of those parties involved and the categories and approximate number of personal data records concerned;
    - the name and contact details of the Data Protection Officer or other point of contact where information can be obtained.
    - describe the likely consequences of the personal data breach;
    - describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Processor shall document all data breaches in accordance with Article 33.5 GDPR, including the facts relating to the personal data breaches, the consequences thereof and the measures taken to correct the respective breach. At Controller's request, Processor shall provide access hereto.

Article 8. Processing requests from parties involved

1. In the event a party involved makes a request to exercise his or her legal rights under the GDPR (Articles 15-22) to Controller, Processor shall pass on such request to

Controller, and Controller shall process the request. Processor may inform the party involved.

Article 9. Secrecy and Confidentiality obligations

1. All personal data that Processor receives from Controller and/or collects itself under this Data Processing Agreement, is subject to strict obligations of confidentiality towards third parties. Processor shall not use this information for any purpose other than for which it was obtained, not even if the information has been converted into a form that is no longer related to an identified or identifiable natural person.
2. The confidentiality obligation shall not apply to the extent Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

Article 10. Audit

1. Controller has the right to conduct audits on Processor through an independent third party who is bound by confidentiality obligations to verify compliance with the security requirements, compliance with data processing regulations, and all issues reasonably connected thereto.
2. This audit may be performed in case a substantiated allegation of misuse of personal data has arisen.
3. Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.
4. The audit findings shall be assessed by Processor and implemented if and to the extent deemed reasonable by Processor.
5. The costs of the audit shall be borne by Processor in case the audit reveals discrepancies with the subjects of clause 1 of this article that are attributable to Processor. In all other cases the costs of the audit shall be borne by Controller.

Article 11. Liability

1. Parties explicitly agree that any liability arising in connection with personal data processing shall be as provided in the Agreement.

Article 12. Term and termination

1. This Data Processing Agreement enters into force by ordering a Service or Ancillary Service via for example the INIZ website.
2. This Data Processing Agreement has been entered into for the duration as specified in the Main Agreement between the Parties, and failing that, at least for the duration of the cooperation between the parties.
3. Upon termination of the Data Processing Agreement, regardless of reason or manner, Processor shall destroy all personal data present to the Processor and remove or destroy any copies thereof.

4. Processor is entitled to amend this Data Processing Agreement from time to time. Processor shall notify the Controller of amendments at least 30 days prior to their taking effect. Controller may terminate if the amendments are unacceptable to Controller.

Article 13. Applicable law and competent venue

1. This Data Processing Agreement and its execution are subject to British (United Kingdom) law.
2. Any disputes that may arise between the parties in connection with this Data Processing Agreement shall be brought to the competent court for the place of business of Processor.

Appendix 1: Stipulation of personal data and data subjects

Personal data

Processor shall process the personal data below under the supervision of Controller, as specified in article 1 of the Data Processing Agreement:

- Names and addresses
- Telephone numbers
- E-mail addresses
- Visitor behaviour
- IP addresses
- Financial data

Of the following categories of parties involved:

- Customers
- Account holders
- Leads and potential customers

Controller represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate, and shall indemnify and hold harmless Process for all faults and claims that may arise from a violation of this representation and warranty.