Evira – Standard Terms for Organisations (Public Sector)

1. PARTIES

Evira provides the Service under these standard terms; optional governance may be agreed at call-off ("the Agreement") and concerns the contracting parties.

1.1. [Clinic name], Org.no. [organisation number], [address] ("the **Clinic**").The Clinic's authorised personnelusing the service are the "the **Healthcare Professionals**".

1.2. Evira Ltd, Org.no 15159570, 5 Upper Montagu Street, London, W1H 2AG, United Kingdom, is from now on referred to as "**Evira**".

The Clinic and Evira are each a 'Party', together the 'Parties'.

2. BACKGROUND

2.1. The Clinic operates care facilities including obesity management services. The Clinic's operation is based on the healthcare agreement in its specific country or region.

2.2. Evira develops and provides a digital platform supporting clinical obesity treatment ("the **Platform**"). The platform is CE-certified (MDR Class-I[1]). In addition, Evira provides specific hardware for this purpose, i.e. obesity treatment.

2.3. Evira's service delivery will be carried out in accordance with the clauses in this agreement, the Data Processing Agreement and appendices which comprises the full agreement package. In case of conflict, the Call-Off Contract prevails over these Standard Terms, and appendices unless stated otherwise.

3. ACCESS TO THE PLATFORM, TERMS AND CONDITIONS FOR USING THE PLATFORM, ETC.

3.1. Evira grants the Clinic access to the Platform for up to the number of clinical user accounts specified in Appendix A for the purpose of providing obesity management services.

[1] https://www.evira.se/doc.pdf

3.2. The Clinic will, through the Platform, gain access to an administrator account, through which the Clinic will be able to administer user accounts for the Healthcare Professionals.

3.3. The user accounts provided to the Healthcare Professionals are unique and specific to each user.

3.4. The Clinic is given access to the Platform during the period of the Agreement and the Agreement can solely be terminated in accordance with section TERM AND TERMINATION below.

3.5. In accordance with the Agreement in each individual case between the Parties, Evira will grant the Clinic the right to use Evira's hardware in accordance with the terms stated in the Agreement.

3.6. Evira shall provide the Clinic with new versions and necessary updates of the Platform, which shall be considered as a part of the Service.

3.7. Evira shall in accordance with the Agreement provide support. Support services can be accessed via e-mail as well as through telephone, via the platform or by other appropriate means of communication. Support shall be offered promptly but within a maximum of three (3) business days. Answers to support questions do not necessarily mean that the issue is resolved or as agreed upon between the Parties.

3.8. Support can be provided in Swedish and English.

4. PROVISION OF BODY SCALES ETC.

4.1. Evira shall provide the Clinic with compatible body scales as specified in Appendix A.

5. RELATIONSHIP TO THE END USERS

5.1. The Clinic has the full responsibility for the care of the Clinic's patients and undertakes to provide information regarding the equipment and all other aspects of the Service, including instructions and care of devices. The Clinic is solely responsible for all clinical decisions and patient care within obesity treatment. Contact between Evira and the patients shall only refer to technical support, unless anything else has been agreed upon between the Parties.

6. THE PARTIES' GUARANTEES

6.1. Evira's Guarantees

6.1.1. Evira shall provide the Service in a professional manner and carry out the Service with the required expertise, speed, cost-effectiveness and care.

6.1.2. Evira undertakes to comply with all the laws and regulations applicable to Evira's provision of the Platform and Evira's services to the Clinic,

6.1.3. Evira shall, at the request of the Clinic, provide information and documentation that may reasonably be required for the Clinic to be able to fulfil its obligations under the Agreement.

6.2. Clinic Obligations

6.2.1. The Clinic undertakes to, for the duration of the Agreement:

a) within the bounds of reasonable care ensure that the Clinic's data and patient data entering the Platform are (i) free from viruses, trojans and any other harmful software or code, (ii) are in the agreed format, and (iii) not otherwise may harm or adversely affect Evira's Platform and the provision of the Service;

b) ensure that access to user accounts on the Platform are solely provided to authorised personnel with a need-to to access such information which is available in the Platform;

c) at each occasion notify Evira which employees at the Clinic shall have access to administration accounts on the Platform;

d) at Evira's request, provide information and documentation which reasonably may be required in order for Evira to meet its obligations in accordance with the Agreement;

e) provide Evira with information concerning planned changes in the Clinic's operations, which can be expected to affect Evira's obligations under the Agreement;

f) perform its duties as healthcare provider responsible for patients adequately;

g) otherwise assist Evira in order for Evira to fulfil its obligations under the Agreement in a professional and effective manner; and

h) ensure that the Clinic has the right to handle the data that the Clinic transfers to the Platform and immediately inform Evira if such right ceases, for example in the event of withdrawal of the healthcare agreement.

7. LIABILITY

7.1. The Service shall be considered defective if the Service deviates from the requirements of the provision of the Service in accordance with this Agreement and if such default causes damage to the Clinic (”a **Default**”).

7.2. Evira is not liable for Defaults in accordance with section 8.1 which constitutes:

a) a Default in third party products;

b) any Defaults caused by the Clinic’s changes or interference with the Platform or the Service;

c) any Defaults caused by the Clinic’s usage of the Service in breach of any provided instructions by Evira or according to the Agreement at given time;

d) any Defaults due to the Clinic not providing correct information, patient data or otherwise providing inaccurate or inadequate system conditions.

7.3. Evira is not liable for any Defaults that are of no significance for the intended use of the Platform and/or the Service and Defaults that do not cause any inconvenience to the Clinic.

7.4. The Clinic shall report a Default in writing to Evira no later than thirty (30) days after the Default has been discovered by the Clinic. The complaint shall contain detailed information concerning the Default.

7.5. Evira undertakes to correct a Default within thirty (30) days from receiving the Clinic’s complaint in accordance with section 8.4.

7.6. If the Clinic has reported a Default and it turns out during Evira’s rectification that no Default existed, the Clinic shall reimburse Evira according to the price list for work performed in regards to the rectification. Evira shall notify the Clinic in cases where this might become relevant in connection with the initiation of the remedial work.

8. LIABILITY AND LIMITATION OF LIABILITY

8.1. If Evira fails to fulfil its obligations under the Agreement and if Defaults or other breaches of the Agreement are not remedied in accordance with what is otherwise stated in the Agreement, Evira shall be liable to pay damages to the Clinic for any direct damages incurred by the Clinic.

8.2. Evira shall in no event be liable to compensate the Clinic for indirect damages, such as loss of profit, loss of production, costs for hiring of consultants, costs for equipment and similar costs or losses, or loss of data. Furthermore, Evira shall not be liable for damages that occur as a result of loss of or faulty material provided or stored by the Clinic through the Platform and/or Service, or any damages that is caused by any authorised or unauthorised person gaining access to, modifying or destroying data or information.

8.3. Evira's liability under the Agreement is, except in cases of intent or gross negligence, limited to an amount corresponding to thirty (30) percent of all fees invoiced by Evira to the Clinic during the preceding twelve (12) months under the Agreement. If the Agreement has not been applicable between the Parties for twelve (12) months, the calculation of the maximum liability shall refer to the sum of all fees invoiced by Evira to the Clinic, divided by the number of months that the invoiced fees covers, multiplied by twelve (12).

8.4. In order for the Clinic to make a claim for damages under the Agreement against Evira, such claim must be brought no later than three (3) months from the Clinic becoming aware of the breach. If the Clinic neglects to submit a written claim within such a time period, the Clinic loses its right to make a claim for damages against Evira relating to such a breach of the Agreement.

8.5. Furthermore, Evira is solely responsible for product liability in accordance with the obligatory provisions of the Swedish Product Liability Act (1992:18). Evira disclaims all other product liability. The Clinic shall, without delay in writing, notify Evira of any damage to property and personal injuries caused by defective products provided by Evira under the Agreement and all claims made by third parties based on such damage and/or risk for such damage. To the extent that Evira incurs liability in relation to third parties, the Clinic shall compensate Evira to the same extent as Evira's liability is limited in accordance with this section 9.

8.6. The Clinic shall hold Evira harmless from any direct damage that Evira suffers due to the Clinic's non-compliance with the obligations under the Agreement, including but not limited to, the Clinic's infringement

in Evira's intellectual property rights or the Clinic's usage of the Platform and/or Service in breach of the Agreement.

9. PROCESSING OF PERSONAL DATA

9.1. The Clinic is the personal data controller in relation to the personal data that Evira may process during the provision of the Service. In the event that Evira processes personal data on behalf of the Clinic when providing the Service in accordance with the Agreement, Evira shall be a personal data processor when processing such data.

9.2. The Parties have, in accordance with Article 28 GDPR, entered into a Data Processing Agreement which regulates the personal data processing that Evira may carry out on behalf of the Clinic.

9.3. Personal data may be shared under confidentiality with employees of Evira who are involved in quality assurance, development of Evira's treatment concept as well as technical support. Pseudonymised personal data may be shared with analysts at Evira, who manage aggregated statistics or evaluate and improve the Service. Pseudonymised personal data are derivatives of personal data that can only be derived to a person with the help of supplementary data. Analysts do not have access to the supplementary data.

10. INTELLECTUAL PROPERTY RIGHTS

10.1. The Clinic does not acquire any ownership, copyright or other intellectual property rights attributable to the Platform or the development thereof. The Clinic acquires only a right to use the Platform in accordance with the provisions of the Agreement.

10.2. The Clinic shall not circumvent any technical limitations of the Platform.

10.3. The Agreement does not affect the Parties' ownership of their respective intellectual property rights acquired or developed prior to the signing of the Agreement, including any subsequent upgrades, modifications and improvements of such intellectual property rights (such as new tools, applications or other methods of visualisation, communication, data collection or analysis).

10.4. The Clinic has the right to use materials and routines provided by Evira for internal use during the period of the Agreement.

10.5. All written material, such as manuals, treatment instructions and teaching materials provided by Evira to the Clinic under the Agreement, whether digitally or in printed form, constitutes the

property of Evira and may not be copied or distributed in any form to another party without the written approval of Evira.

10.6. The Clinic grants Evira a non-exclusive license to use the Clinic's data that may be processed, handled and/or treated by Evira during the provision of the Service to deliver and to develop the Service. Evira does not claim any intellectual property right, or property right of any kind, to the Clinic's data.

10.7. Evira obtains the right to save anonymised derivatives of data. Anonymised data may be shared with third parties for research purposes. The regulations on data protection are not applicable for anonymised data due to the fact that personal data cannot be identified.

11. TERM AND TERMINATION

11.1. This Agreement enters into force when signed by the Parties and remains in force until terminated in accordance with this Agreement, unless otherwise agreed in the Call-Off Contract..

11.2. Each Party is entitled to terminate the Agreement with immediate effect if the other Party:

11.2.1. is the subject of a proceeding in bankruptcy, insolvency or other law of the relief of debtors, including the appointment of any receiver or trustee or assignment for the benefit of creditors; or

11.2.2. commits a material breach of its obligations pursuant to this Agreement and, if rectification is possible, does not rectify it within ten (10) Business Days of notification of such breach by the non-defaulting Party.

11.3. If the Clinic's healthcare agreement ends, the Clinic has the right to terminate the Agreement with immediate effect as long as the Clinic has kept Evira informed of the current processes that led to the termination, otherwise the notice period applies. The Clinic is obliged to immediately inform Evira if a change takes place regarding these agreements that affect Evira's situation.

11.4. A Party's notice of immediate termination in accordance with above sections shall be given without undue delay after such a circumstance that gives rise to such a notice becomes known to the terminating Party.

11.5. Termination of this Agreement will be without prejudice to any rights and obligations of any Party against the other Party which may have accrued up to the date of such termination.

11.6. For avoidance of doubt, it shall be noted that the Clinic's access to the Platform shall cease upon termination.

11.7. Agreement provisions on confidentiality, dispute, intellectual property rights and information ownership applies even after the Agreement in other aspects has ceased to apply.

12. CONFIDENTIALITY

12.1. Save for the other Party's prior written consent, each Party hereby undertakes not to directly or indirectly exploit or reveal to a third party any information about this Agreement or confidential information that a Party has received as a result of or pursuant to this Agreement. The Parties are strictly liable for ensuring that its employees meet these undertakings and that confidential information is not being spread to other employees than those in need of the information to fulfil the rights and obligations under this Agreement.

12.2. Confidential information refers to (i) all non-publicly available information about a Party's services, products, offering, prices, or end customers/users, (ii) information about tools and methods for processing data (including know-how), (iii) information that may not be disclosed by law and (iv) any other information that the receiving Party should reasonably understand is confidential by the nature of that information or any labelling.

12.3. This confidentiality obligation shall not prevent a Party from disclosing information in the manner and to the extent required by applicable laws and regulations or by a decision of an authority or a court.

12.4. The confidentiality commitments of the Parties under this section shall continue to apply without limitation in time after the termination of the Agreement.

12.5. Upon request and/or upon termination of the Agreement, a Party shall, at the request of the other Party, return or destroy all material containing confidential information regarding the other Party. This does not apply to such information which is necessary for a Party to be able to exercise its intellectual property rights or fulfil its obligation under applicable law.

12.6. Confidentiality obligations are subject to statutory disclosure requirements, including FOIA. If disclosure request received, Party shall notify the other Party to allow objections where legally possible.

13. CONSEQUENCES OF TERMINATION OF THE AGREEMENT

13.1. Upon termination of the Agreement, access to the various hardware provided by Evira shall cease and the Clinic shall return such hardware to Evira at the Clinic's expense and within 3 months from termination.

13.2. The Clinic has no obligation to return any hardware that has been duly handed out to patients in accordance with current terms and routines at new registrations.

13.3. The Parties shall establish a plan for the decommissioning of the products and Services offered by the Parties, designed so that it minimises, as far as possible, the disruptions that a decommissioning may entail for end users and patients.

14. FORCE MAJEURE

14.1. If a Party would be prevented from fulfilling their obligations under the Agreement due to circumstances beyond the Party's control which the Party could not have foreseen or taken into consideration prior to entering the Agreement and whose consequences the Party could not reasonably have avoided or overcome, this shall be grounds for exemption from liability for damages.

14.2. Party who asks for relief from a ground for exemption according to the above paragraph shall immediately inform the other Party, and describe the ground for exemption and specify its assessment for when the ground for exemption is expected to cease. A Party is entitled to terminate the Agreement with immediate effect, if performance of a contractual obligation is prevented for a period of three (3) months or more, due to circumstances beyond the other Party's control.

15. MISCELLANEOUS

15.1. Any notices and other communication made under or in connection with this Agreement must be in writing, and must be sent by courier, registered or certified mail or email and be addressed to the other Party as set forth in this Agreement or to such other address as a Party may notify the other Party in accordance with this section by not less than five (5) business days' notice in accordance with this section 17.1

15.2. No Party may assign, transfer or pledge or otherwise dispose of or grant any security interest in or over any of its rights or obligations under this Agreement without the prior written consent of the other Party. The Parties have the right to hire subcontractors for the fulfilment of their obligations under the Agreement. The Parties are responsible for the sub-contractor in relation to the other Party.

15.3. Alterations and additions to this Agreement shall be done in writing and signed by both Parties.

15.4. The Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior agreements and understandings, both written and oral.

15.5. Should any provision in the Agreement, or part thereof, prove to be invalid, this shall not mean that the Agreement in other aspects is invalid. Instead, the Parties shall in good faith negotiate and decide on such adaptation of the Agreement as is required in order to achieve a regulation that, as far as possible, achieves the legal and commercial effect that the Parties intended with the original provision.

16. GOVERNING LAW AND JURISDICTION

16.1. This Agreement, including all Call-Off Contracts, appendices and the Data Processing Agreement, shall be governed by and construed in accordance with Swedish law.

16.2. For Clinics that are not public-sector entities, any dispute, controversy or claim arising out of or in connection with this Agreement shall, as a main rule, be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (SCC), with the seat of arbitration in Stockholm, Sweden.

16.3. Notwithstanding the above, if the Clinic is a public-sector entity or otherwise subject to mandatory rules that restrict or prohibit arbitration, disputes shall instead be settled by the competent courts of Sweden, with the Stockholm District Court as the court of first instance.

16.4. Nothing in this section shall prevent a Party from seeking interim or injunctive relief before a competent court.

16.5. The language to be used in the arbitral proceedings shall be English unless otherwise is agreed upon by the parties.

16.6. The Parties agree not to disclose any information obtained in connection with the arbitration proceedings (including all

communications, decisions and rulings in the arbitration proceedings) to any third party unless the other Party has given its written consent to disclose such information or if required to do so by law or other binding regulations.

16.7. This section on governing law and jurisdiction shall not prevent a Party from providing such information in order to safeguard its rights vis-à-vis the other Party or third parties in connection with the dispute, providing information that the Party is obliged to provide according to applicable law, authority decision, court decision, arbitration, or agreement with the stock exchange or other marketplace on which the Party (or its direct or indirect parent company) is listed or if the information is already public without the Party having breached its obligations under this Agreement.

---

17. Appendix A

1. PROVISION OF BODY SCALES AND OTHER DEVICES.

    a. Evira shall provide the Clinic with a standard maximum entitlement of three (3) body scales per two (2) patients. This so the Clinic will be able to provide some patients with several scales, since the patients may live with different caretakers, and for the Clinic to be able to replace equipment that has been damaged due to incorrect use. Evira may also provide activity trackers to certain patients.

    b. Evira undertakes to, within three (3) weeks notice, continuously during the period of the Agreement deliver equipment to the Clinic in accordance with Appendix A. This in accordance to the number of patient accounts agreed upon between the Parties. Deliveries can be requested at least fourteen (14) days apart but not more frequently. Evira has the right to decide the number of body scales delivered each time. The Clinic undertakes to store and administer the equipment for the patients between deliveries.

2. Evira grants the Clinic access to the Platform for up to [number of] clinical user accounts.

3. Further commercial terms are agreed in the Call-Off Contract.

Data Processing Agreement

Table of contents

1 Parties

1.1 Based on the Standard Contractual Clauses with modifications of the *third-party beneficiary clauses* and *erasure and return of data* for the purposes of Article 28(3) of Regulation 2016/679 (the GDPR), these Contractual Clauses (the "**Clauses**") are agreed upon between:

Data controller	**Data processor**
[Company name]	Evira Ltd
[CVR]	15159570
[Address]	5 Upper Montagu Street
[Zip code]	W1H 2AG London, England

in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1.2 The above-mentioned Parties are hereinafter jointly referred to as the "**Parties**", or individually as a "**Party**".

2 Preamble

2.1 The Clauses set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) GDPR on the protection of natural persons with regard to the processing of personal data.

2.3 In the context of the provision of the platform Evira and related services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses. The Clauses are only complete together with the attached four appendices.

2.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3 The rights and obligations of the data controller

3.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU, Member State[1] or UK data protection provisions and the Clauses.

3.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4 The data processor acts according to instructions

4.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by EU, Member State or UK law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU, Member State or UK data protection provisions.

5 Confidentiality

5.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6 Security of processing

6.1 Article 32 GDPR stipulates that, 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 natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks

require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7 Use of sub-processors

7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller in writing of any intended changes concerning the addition or replacement of sub-processors at least one month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU, Member State or UK law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7.6 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8 Transfer of data to third countries or international organisations

8.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU, Member State or UK law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a. transfer personal data to a data controller or a data processor in a third country or in an international organisation

b. transfer the processing of personal data to a sub-processor in a third country

c. have the personal data processed in by the data processor in a third country

8.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9 Assistance to the data controller

9.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject,

b. the right to be informed when personal data have not been obtained from the data subject,

c. the right of access by the data subject,

d. the right to rectification,

e. the right to erasure ('the right to be forgotten'),

f. the right to restriction of processing,

g. notification obligation regarding rectification or erasure of personal data or restriction of processing,

h. the right to data portability,

i. the right to object, and

j. the right not to be subject to a decision based solely on automated processing, including profiling.

9.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3, the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10 Notification of personal data breach

10.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2 The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. 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.

10.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11 Erasure and return of data

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless EU, Member State or UK law requires storage of the personal data or unless the return of the personal data has been requested in writing by the data controller.

12 Audit and inspection

12.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

12.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities,

or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13 The parties' agreement on other terms

13.1 The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14 Commencement and termination

14.1 The Clauses shall become effective on the date of both parties' signature.

14.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15 Signature

On behalf of the data controller
Location and place:
[Location, date]

[Company name]
[Signer name]
[Signer position]
[Signer phone number]
[Signer email]

Signature:

[Signer name]

On behalf of the data processor
Location and place:
[Location, date]

Evira Ltd
[Signer name]
[Signer position]
[Signer phone number]
[Signer email]

Signature:

[Signer name]

16 Data controller and data processor contacts/contact points

16.1 The parties may contact each other using the following contacts/contact points:

16.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Data controller contact
[Contact name]
[Contact position]
[Contact phone number]
[Contact email]

Data processor contact
[Contact name]
[Contact position]
[Contact phone number]
[Contact email]

Appendix A · Information about the processing

A.1 The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the data processor's processing of personal data on behalf of the data controller is to help the data controller in their work with behavioural obesity treatment. The purpose entails the following parts:

1. Manage user accounts (user accounts and administrative accounts)
2. Relay communication between user accounts and administrative accounts
3. Store and preserve data related to the user and administrative accounts
4. Analyse data related to the user and administrative accounts to generate reports to the data controller
5. Analyse data related to the user and administrative accounts to generate recommendations to the data controller
6. Analyse data related to the user and administrative accounts to generate recommendations to the users on behalf of the data controller

The data controller might also ask the data processor to perform additional managerial tasks from time to time including transfer of data to national quality registers or to appointed clinical research staff. The frequency and magnitudes of such tasks must be aligned with the commercial agreement between the parties.

The data processor also takes responsibility to record and to store complete access logs and edit histories in accordance with data accessibility guidelines.

A.2 The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The nature of the processing includes recording, collecting and storing data added directly by users or by the data controller, organising and structuring said data to generate recommendations and aggregations, and retrieving data, recommendations and aggregations to both user and administrative accounts.

A.3 Processing includes the following categories of data subject:

1. Administrative accounts
   There are different types of administrative accounts
   a. Administrator accounts are used to add or remove user accounts (patient/family accounts) as well as access other tools and services that the Platform provides.

b. Clinic administrator accounts can, in addition to what an Administrator account can, also add or remove Administrator accounts.

c. Support administrator accounts are used by the data processor and can access the entire Platform (clinic data and patient data) and thus manage all types of administrative accounts. This account type is used by the data processor for technical support and quality control by instruction of the data controller.

2. User accounts
   User accounts are used by patients and family members or other related individuals that the patient (and if applicable guardians) and the data controller deem reasonable to include in the intervention.

A.4 The processing includes the following types of personal data about data subjects:

1. User accounts

   a. name;
   b. NHS number;
   c. sex;
   d. e-mail address;
   e. phone number;
   f. health information (weight, height);
   g. health information that may occur in the communication between the Clinic and it's patients and internal communication within the Clinic;
   h. health data (information that is registered through an activity bracelet, scale and from analyses based on behavioural patterns and surveys);
   i. browser storage such as cookies, session storage and local storage;
   j. IP-address;
   k. if the user is a patient or a family member;
   l. what clinic the user is connected to;
   m. if the user is in active treatment;
   n. account activity history from access logs;
   o. derived data including when the user has visited the clinic, when the user has been active in the app or recorded information; and
   p. other data, including health data, that the data controller instructs the data processor to process in relation to clinical trials or other projects overseen by competent authority.

2. Administrative accounts

   a. name;
   b. professional title;
   c. date of birth;
   d. e-mail address;
   e. phone number;
   f. IP-address;

g. what clinic the user is connected to;
h. if the account has administrative rights; and
i. account activity history from access logs.

A.5 The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

1. Administrative accounts
   Administrative accounts are used by the data controller to access the service. Some information about administrative accounts will be stored for an extended period of time (ten years) in the form of access logs.

   If the data controller deems storage of access logs unnecessary the data processor will comply. Historic access logs can at any time be transferred to the data controller and thus not be stored by the data processor.

2. User accounts
   The main rule is that personal data relating to user accounts is stored for the duration of participation. Participation can be both active and paused.

Appendix B · Authorised sub-processors

B.1 Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

SUB-PROCESSOR	SUB-PROCESSING LOCATION	DESCRIPTION OF PROCESSING	TRANSFER MECHANISM
Microsoft AB Regeringsgatan 25, 111 53, Stockholm Sweden VAT Reg. No. SE556233480401	EEA	Providing and maintaining servers for processing and storing data	N/A EC Adequacy decision
Infobip RN: 7085757 5th floor, 86 Jermyn Street, SW1Y 6AW London, United Kingdom	UK, EEA	Service provider for sending text messages (SMS) and e-mails	N/A EC Adequacy decision
Scaleway SAS Scaleway SAS BP 438 75366 - Paris CEDEX 08 France	EEA	Providing and maintaining servers for processing and storing data.	N/A
Google Ireland Ltd Gordon House Barrow Street Dublin 4 D04E5W5 Ireland	EEA	Sending notifications to users' smartphones (Firebase)	N/A

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2 Prior notice for the authorisation of sub-processors

See Clause 7.3.

Appendix C · Instruction pertaining to the use of personal data

C.1 The subject of/instruction for the processing

See A.1

C.2 Security of processing

The level of security shall take into account that the processing involves personal data which are subject to Article 9 GDPR on 'special categories of personal data' which is why a 'high' level of security will be established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Pseudonymisation and encryption

a. personal data is to be encrypted in transfer and at rest;

b. the availability of personal data should be limited and scoped to a bare minimum when possible;

c. personal data should be pseudonymized whenever possible by removing personally identifiable data such as name, address, phone number, email, civil registration number and IP-address. The data should instead be identified by a randomised identification number;

Requirements for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

d. storage systems and servers are to be selected among internationally recognized and trusted providers to ensure a high degree of security, confidentiality and resilience;

e. storage systems are periodically backed up in so-called "backups" to ensure availability. Each backup may only be stored for a maximum of 30 days;

Requirements for regular testing, assessing and evaluating effectiveness of technical and organisational measures for ensuring security of processing

f. the data processor's software shall be subject to adequate and continuous testing, both automatic and manual, in order to guarantee safe usage and security;

g. the data processor's software shall be subject to external security verification and penetration testing from established security consultants from time to time;

h. the data processor guarantees to maintain due internal security routines for data management, key management, and other tasks related to data processing and storage given the sensitive nature of the data;

i. the data processor's internal security routines are to be revised annually at a retrospective in order to continuously improve security routines;

Access controls for data online

j. data can only be accessed by authenticated and authorised personnel;

k. users can only access their data when authenticated;

l. two factor authentication per default;

m. the degree of authentication is determined by the sensitivity of the data;

Requirements for protection of data during transmission and storage

n. all digital communications must be encrypted according to modern web standards

o. all digital data access requires token-based authentication with expiring tokens

Logging

p. the data processor will record and log any and all access to data (*access logs*)

q. application logs are only stored for a short time period in order to enable application performance analysis, debugging, and security oversight; while not being persistent in order not to store sensitive data

Organisational measures

r. access to personal data for the data processor's employees shall be limited to only those employees who need access to fulfil their respective duties;

s. the data processor shall have established routines and processes to train its employees to protect the personal data against unauthorised access;

C.3 Assistance to the data controller

The data processor shall insofar as this is possible assist the data controller in accordance with Clause 9.1. and 9.2.

C.4 Storage period/erasure procedures

The data processor shall remove data after instructions from the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

The data processor saves anonymised derivatives of the data. Data protection regulations do not apply to anonymized data as it cannot be used to identify a person.

C.5 Processing location

Processing of personal data will be performed in the EEA. Processing may also be carried out in the UK. For data controllers under the EU GDPR such UK processing should immediately be cancelled if the European Commission changes the relevant adequacy decision. See list of sub-processors.

C.6 Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7 Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall three months after the controller's request obtain an inspection report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU, Member State or UK data protection provisions and the Clauses at the data controller's expense.

The report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU, Member State or UK data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

C.8 Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor or the data processor's representative may perform a physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU, Member State or UK data protection provisions and the Clauses.

In addition to the planned inspection, the data processor may perform an inspection of the sub-processor when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU, Member State or UK data protection provisions and the Clauses.

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU, Member State or UK data protection provisions and the Clauses.

Appendix D · The parties' terms of agreement on other subjects

D.1 Other subjects

The data processor relies on the personal data processed on behalf of the data controller for billing purposes. The data controller thereby disclaims all rights to challenge the specificities of previous bills when instructing the data processor to remove or alter the underlying data unless the instructions to remove data are motivated by the data processor's breach of contract.