INFORMATION DOCUMENT AND RECORD OF PROCESSING ACTIVITIES

Drafted on: 16 May 2015
Updated on: 4 January 2019

EU General Data Protection Regulation (679/2016)

1. Data controller	**Aava Virta**
2. Person in charge of the data file Contact person	Petteri Kilpinen, Business director Annankatu 34-36 B, FI-00100 Helsinki, Finland tel. +358 (0)10 380 3800 (firstname.lastname@aava.fi) Päivi Sotkas, Unit Manager Annankatu 34-36 B, FI-00100 Helsinki, Finland tel. +358 (0)10 380 3800 (firstname.lastname@aava.fi)
3. Data protection officer	Ida-Emilia Laasonen Annankatu 32, FI-00100 Helsinki, Finland tel. +358 (0)10 380 3800 dpo@aava.fi
4. Name of the data file	**Centralised customer register of Aava Virta, and its self-employed partners.**
5. Purpose of the processing of personal data and purpose of the data file Purpose of maintaining the data file	The principal purposes of the data file are to determine the state of health and well-being of customers, to plan, implement and monitor well-being coaching sessions, and to process any related information. The register is also used for invoicing and collection purposes as well as for maintaining customer relationships. Furthermore, the register is used for planning, developing, compiling statistics and following up of the data controller's own operations as well as for tasks related to the implementation of the rights and obligations of the data controller. The primary basis for processing personal data is the relationship between the customer and Aava Virta, customer's consent, assignment from the customer or other appropriate connection.
6. Content of the data file	Only essential data is collected in the register. Collected data may include, as necessary: • First and last name • Personal ID number • Address • E-mail address • Employer information • Gender, height and weight • Activity class, maximum and minimum heart rate, maximal oxygen intake • Diseases and medication • Other information related to state of health and well-being provided by the customer • Results of well-being survey and analysis and reports generated according to them • Reports and training programmes prepared by the coach. Name and title of the person who made the entry and date of entry.

7. Regular sources of data	Data provided by the customer. Data, reports and feedback related to well-being measurements. Documents obtained from other treatment or rehabilitation units with the permission of the customer.
8. Regular disclosure of data	Customer data may be disclosed to the person concerned, if there are no legislative reasons that would prevent it. To third parties with the written consent of the person in question. Information necessary for the purpose of arranging the examination and treatment of a customer may be given to another health care unit or health care professional. Information in the customer register is disclosed to authorities, such as the Parliamentary Ombudsman, The National Supervisory Authority for Welfare and Health, Regional State Administrative Agencies as well as insurance institutions, based on the special provisions set forth in the legislation. The aforementioned organizations process the confidential data disclosed to them in order to carry out their statutory duties and only for the purposes specified by law. In addition, information in the customer register may be disclosed, regardless of any secrecy obligation, to authorities maintaining national registers, such as the cancer and infectious disease registers maintained by the National Institute for Health and Welfare and the Adverse Reaction Register maintained by the Finnish Medicines Agency Fimea. It is also to be stated that a copy of the well-being survey is delivered to specified maintenance system suppliers in an anonymised format for statistical research purposes—for example, for calculating average reference ranges. Personal data is disclosed, when necessary, to credit management and invoicing service providers for reminder and collection purposes. The data is always disclosed according to the Data Protection legislation and within the limits laid down by it.
9. Transfer of data outside the EU or the European Economic Area	The data in the data file will primarily not be disclosed outside the European Union or the European Economic Area. The personal data of the data subject may be transferred outside the EU or EEA only with the data subject's specific consent or in exceptional cases to protect the vital interests of the data subject.
10. Storage, filing and disposal	Personal data is stored in the Aava Virta personal data register until the customer relationship of the customer and Aava Virta can be considered as terminated. The termination time will be defined by adding five years to the last service contact or contact. Personal data is disposed of so that unauthorised persons cannot access the data.
11. Systems used in processing	The following systems are used when processing personal data: - Aerolution physical fitness analysis (Health Visor Oy) - DynamicHealth – patient information and operational activities

	management information system (Tieto Oyj) - Firstbeat (Firstbeat Technologies Oy) - Inbody (Bittium Biosignals Oy) - K5 – test equipment - Mywellness Cloud (Qicraft Finland Oy/Technogym S.p.A) - Webropol survey tool (Webropol Oy) - Event management tool Lyyti (Lyyti Oy)
12. General description of technical and organisational security measures	Aava Virta protects the entire lifecycle of the personal data using appropriate safeguards. Personal data is protected, for example, by predictive risk management, electronic safeguards, back-up copying, user management and security systems. Training and instructions were provided to employees when the software was deployed. IT support and main users were trained more extensively. New employees are trained and receive instructions as part of their job orientation. All employees sign a non-disclosure agreement at the time of signing their employment contract. The non-disclosure agreement remains valid after the termination of the employment relationship. Manual documentation shall be stored in lockable archives, and only the persons who have the right to access them on the basis of confidentiality rules may access the documentation. Electronically stored data is protected through electronic access rights. Software applications and workstations require personal user credentials. Usage of data systems and the access to the data in them is monitored separately for each username.
13. Right of access and realisation of the right of access	Regardless of secrecy provisions, customers shall have the right of access to the data on them in a personal data file. The right of underage persons to obtain information on themselves is determined according to general provisions on the right to be heard. Underage persons who are under 15 years of age but, in the view of their age and maturity, are capable of making decisions on their treatment, may exercise the right of access independently. If an underage person who is capable of making decisions on treatment forbids the disclosure of the data to a parent or guardian, the latter shall have no right of access to customer register data. The request to access customer data shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The identity of the persons exercising their access right shall be verified. Customers have the right to access their own records and obtain their information in writing on request. The access shall be provided without unnecessary delay, and the data shall be provided in a legible form. If necessary, a healthcare professional may explain the data.
14. Rectifications and their implementation	The controller shall, on its own initiative or at the request of the customer, without undue delay rectify, erase or supplement any data contained in the data file if it is erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing. A request for rectification shall be made in writing to the Accunt manager of the Well-being Services. The identity of the persons exercising their access right shall be verified.

	The decision shall be made by the responsible coach or tester. If the responsible coach or tester no longer works for the unit, the request is made to the person responsible for register affairs, who will make the decision on approving the rectification request.
15. Right to erasure (“right to be forgotten”)	The customer has, under certain conditions, the right to have their data erased, also known as the right to be forgotten. The customer has the right to withdraw consent for the processing of their data and, after that, the right to submit a written request for the erasure of their data to Aava Virta insofar as the data is not processed in order to fulfil a legal obligation. The withdrawal of consent for the processing of personal data and the request for the erasure of personal data shall be made when visiting a clinic in person or by submitting a document that carries the person’s own signature or is otherwise reliably verified. The identity of the person submitting the request shall be verified.
16. Right to data portability	The customer has the right to receive their data from the controller in a machine-readable format and to transmit the data to another controller. However, this requires that the customer themselves has provided the data in question to Aava Virta. The request shall be made when visiting a clinic in person or by submitting a document that carries the person’s own signature or is otherwise reliably verified. The identity of the person submitting the request shall be verified.
17. Right to lodge a complaint with a supervisory authority	The customer has a right to lodge a complaint with a supervisory authority if he/she considers that the processing of the personal data related to him/her infringes the General Data Protection Regulation.
18. Any other rights	The information contained in the centralised customer register of Aava Virta is confidential. Data subjects do not have to expressly prohibit the disclosure of their data. A data subject has the right to prohibit the controller to process personal data for purposes of direct advertising, distance selling and other direct marketing, market research and opinion polls.
19. Register administration	This information document and record of processing activities has last been updated on 4 January 2019. The data controller keeps track of the changes in the legislation and instructions by the authorities concerning data protection and develops the operations of the service. This requires the data controller to reserve the right to update this record.