PRIVACY POLICY OF [ENTER YOUR COMPANY NAME]- FIRSTBEAT LIFESTYLE ASSESSMENT SERVICE

[THIS template is provided as a sample only for Firstbeat Lifestyle Assessment Service Provider customers. You as Controller are fully responsible for validating the content and evaluating its suitability for informing your clients in accordance with your local jurisdiction, and keeping it up to date for example in case of any changes to the legislation, the processing of data or the service. Use a legal expert if needed.

Read the instructions in all yellow comments and remove those comments after updating the privacy policy. If necessary, you may also otherwise update the template text, as long as it accurately describes your service and data processing. We don't recommend changing the parts related to processing by Firstbeat. Read and understand the entire privacy policy.

You can use this policy to inform your users and clients or create similar documentation based on the information in this policy.]

Description of personal data processing in the Lifestyle Assessment service ("Service") produced by [ENTER COMPANY NAME] based on the web service platform provided by Firstbeat Technologies Oy. This document contains information about the personal data processing as required by the EU General Data Protection Regulation (GDPR).

DATA CONTROLLER AND PROCESSOR

"Controller": [ADD your company name, address, business ID or other necessary information] [You may replace this term with your company name in this document, if you want to make it more readable]

"Processor" or "Firstbeat": Firstbeat Technologies Oy (business ID 1782772-5), address Yliopistonkatu 28 A, 40100 Jyväskylä, Finland. Firstbeat acts as personal data processor on behalf of the Controller.

TERMS

"Customer" is a person or organization who is in a contractual relationship with Controller for Controller to produce the Service, using personal and measured information from the Subject(s), who are defined by the Customer. In a typical scenario the Customer is an employer, whose employees are Subjects.

"Subject" is the person, whose information is used by Firstbeat to produce the Service, using pulse measurement data and other personal information about the Subject.

CONTACT PERSON FOR THE DATA CONTROLLER

The data Controller can be contacted at [ADD company e-mail, telephone or other necessary contact information]. The contact person for information security matters is [add contact person name].

THE PURPOSE AND LEGAL BASIS OF PROCESSING THE PERSONAL DATA

[For example:] The purpose for processing personal data in the Service is to provide a personalized analysis to the Subject on the effect of lifestyle factors on different aspects of well-being. The Subject's personal qualities and measured heartbeat analysis data are used to provide the Service. Other purposes include user support activities and statistics on the Service usage.

If the applicable legislation requires the Subject consent for processing some of the personal data described in this document (for instance, concerning health related data i.e. so-called special categories of data), the consent will be acquired using an appropriate method. This may be done for example by checking a separate consent checkbox, making the choice in the technical settings of the service or website, or by another specific action or statement to signify consent. Declining consent may impact the ability to offer the specific service.

Log data of the service use or handling measurement devices is additionally saved in order to protect the legitimate interests of the Controller, Customer, Firstbeat and the Subjects, for example in order to investigate possible security breaches or for example in order to be able to prove, that invoiced services have been delivered.

It shall be noted that Firstbeat gets a copy of data saved in the service in anonymized format for statistical and scientific research, such as for determining average reference values.

[Describe the legal justification in your company and jurisdiction, for example like this:] The legal justification for handling personal data is fulfilling the contract between the parties or the legitimate interest of the Controller, which is based on the relationship between the parties. The legal justification may also be the Subject consent, if the applicable legislation requires this.

[ADD HERE your organization's any other purposes for the data, such as information/marketing, occupational health etc. and the possible other legal justifications related to these purposes]

THE PERSONAL DATA RETENTION PERIOD

[DEFINE the rules applied by your organization for the personal data retention. Ensure, that the personal data is removed in the way you describe.]

[EXAMPLE, check if this applies to your organization and update] Unless otherwise agreed, the personal data related to the measurement will be kept for [fill: XX, for example 24] months after the last measurement to the Subject, as reference for possible follow-up measurements which belong to the service concept, and subsequently erased. If the Subject has given a separate consent for a longer term retention, the personal data may be kept longer accordingly.

DESCRIPTION OF THE GROUP OF DATA SUBJECTS

The personal data from participating Subjects is processed in the Service. In a typical case, the Customer of Controller is the organization represented by the Subjects, often an employer, and the Customer determines the group of Subjects.

REGULAR DATA SOURCES

[ADD your data sources. For example like this]: The Customer provides Controller the email address of each Subject. Each Subject is then emailed a personal web link to activate the Service. The other personal data is provided by the Subjects themselves via the web interface and through the use of measuring devices. A representative of Controller may additionally gather information from the Subjects when providing the Service.

THE TYPE OF PERSONAL DATA

The database contains the following information (partial or complete) about the Subjects:

* Full name (first and last)
* Date of birth, gender, height, weight
* Activity class, maximum and resting heart rate, maximal oxygen

consumption

* Information about chronic diseases and medication provided by the Subject
* Heart rate measurements, acceleration information and diary entries created by the Subject during the measurement period, e.g. alcohol consumption, current and recent illnesses and medications, self-documented events noteworthy of interest to the Subject.
* Contact information, e.g. address, email address and telephone number
* Information about the employer, e.g. name, contact information and personnel

group

* Information about the use of the service
* Information about the consents of processing data in the service
* The results report with defined target actions created for the Subject based on the data analysis

 [NOTE: Some versions of the Service may be possible to use anonymously using a nonpersonal ID chosen by the Subject or Controller. If your organization offers this possibility to the Subject, you can mention this here.]

PRINCIPLES OF DATA PROTECTION

The Controller follows the best practices for managing data, including appropriate technical and organisational measures as required by the personal data legislation. Controller protects the data so that only the authorized personnel defined by Controller, who are bound by confidentiality agreement, have access to the data and only for purposes related to their work. [DESCRIBE, if needed, your data protection practices in more detail: for example, if you save data is additionally saved on employees' workstations, email, network drives, your organization's own applications etc. and potential use of subscontractors]

Firstbeat is for its own part responsible for the protection of the data related to the processing of the information in Firstbeat's systems.

TRANSFER OF PERSONAL DATA

[DESCRIBE any transfer of personal data. Mention for example any transfers agreed with occupational health care. For example: ] Personal data is stored only in systems managed by Controller or Firstbeat. Personal data may not be transferred without the data Subject's consent outside Controller or its present or future subsidiary companies in a manner that the data could be identified connected to an individual person, except in following exceptional circumstances: if required by any ruling of a governmental or regulatory authority, court, or by mandatory law; or if it is otherwise necessary for the purposes of preventing, or investigating, any breach of law, user terms or good practices or to protect the rights of Controller or a third party.

Personal data of the Subjects may be processed by authorized third parties, who process the data on behalf of the Controller for the purposes described in this document (for instance, service providers of technical infrastructure or services). Such service providers may use the personal data only according to the instructions from the Controller, i.e. only for the purpose for which the data has been collected. The Controller requires that the service providers operate according to the applicable legislation and this privacy policy, ensuring appropriate security for the personal data.

[EXAMPLE, verify if this applies in your organization]: Personal data of the Subjects will not be given to the Customer. The Customer only receives average information about their Subject group's wellbeing as a whole. The averages will not be provided if the number of Subjects is so small, that individual data could be recognized from the averages.

[DESCRIBE information whether or not personal data is transferred in your organization outside EU area, for example if you use non-EU cloud services to manage customer information related to this service. Also verify the text below.]

When personal data is processed in Firstbeat's systems it is primarily stored on Firstbeat servers located in the [CHECK which Firstbeat server your account is set up for and modify this accordingly. If your link begins with "lifestyle-uk", it is in the UK server, otherwise it begins with "lifestyle-global" which is in the EU.] EU or the United Kingdom (UK). The Subject may also use the Service with a device outside the EU or the EEA, and in such cases, the data is visible on that device while using the Service.

THE RIGHTS OF THE DATA SUBJECT

The data Subject has the rights according to the personal data legislation applicable in Finland [and ADD your country, if needed], including the EU General Data Protection Regulation (GDPR), to inspect his/her personal information, change or request to change his/her information and under some circumstances, the right to request erasure of personal information. Therefore, the Subject has the right to request the Controller to correct inaccurate or incorrect personal information without unnecessary delay. The Subject has the right to request erasure of his/her information without unnecessary delay, for example when the personal data is no longer required for the original purposes, the personal data has been processed unlawfully, or the Subject withdraws consent to the processing and when there is no other legal ground for the processing.

The Subject has the right to request the Controller to limit the processing in certain situations, including when the Subject denies the information being accurate or the processing is illegal. Under some circumstances the Subject also has the right to object to the processing.

The Subject may, under some circumstances, have the right to request transferring the personal data from one system to another. Whenever the legal justification for processing the personal data is consent, the Subject also has the right to withdraw the consent at any time.

The Controller wishes that any disputes concerning the processing of personal data are primarily resolved in a conciliatory manner between the parties. The Subject has the right to lodge a complaint to the authorities responsible for personal data protection.

[CHECK, and if necessary, update and add the practices in your organization]

Any requests to inspect, modify or erase the personal data shall be indicated to Controller in person, or by a signed letter or similarly verified document, so that Controller can confirm the requestor has the right to make such a request. The request can be made with e-mail, if using the e-mail address registered when using the service. Controller may need to identify the Subject and ask for additional information in order to fulfil this kind of requests.

This description of the personal data processing has been updated [ADD DATE]. Controller follows the changes in legislation and regulator instructions related to personal data processing and develops the service further and will therefore reserve the right to make changes to this description.