Data Processing Agreement

Between:

Data controller

BP1 Első Ütem Zrt.
Contact person: bpowell@futurealgroup.com

and

Data processor

EasyPractice ApS
Strandlodsvej 44, 3. sal
2300 København S
VAT number: 35642536
Contact: kontakt@terapeutbooking.dk

Content

Background for the Data Processing Agreement

- This agreement sets out the rights and obligations that apply when the data processor handles personal data on behalf of the data controller.

- The agreement is designed for the parties to comply with Article 28, piece 3 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (Data Protection Regulation), which sets specific requirements for the content of a data processing agreement.

- The data processor's processing of personal data is done in order to fulfill the parties' "main agreement": the data controller's use of the EasyPractice System.

- The Data Processing Agreement and the "main agreement" are interdependent and can not be terminated separately. However, the Data Processing Agreement may - without terminating the "main agreement" - be replaced by another valid data processing agreement.

- This data processing agreement takes precedence over any similar provisions in other agreements between the parties, including the "main agreement".

- For this agreement there are four appendices. The attachments act as an integral part of the data processing agreement.

- The Data Processor's Appendix A contains details of the treatment, including the purpose and nature of the treatment, the type of personal data, the categories of registered and duration of treatment.

- The Data Processor's Appendix B contains the data controller's conditions for the data processor to make use of any sub-processors, as well as a list of any under-processed data that the data controller has approved.

- The Data Processor's Appendix C contains further instruction on the processing by the data processor on behalf of the data controller (subject matter of the processing), which minimum security measures should be observed and how the data processor and any subdatabases are supervised.

- The Data Processing Agreement Appendix D contains the parties 'possible regulation of conditions, which are not otherwise stated in the data processing agreement or the parties' "main agreement".

- The data processing agreement and its supporting documents are stored in writing, including electronically by both parties.

- This data processor agreement does not release the data processor for any obligations that are directly imposed on the data processor under the Data Protection Regulation or any other law.

The data controller's obligations and rights

- The data controller is responsible for the processing of personal data within the scope of the Data Protection Act and the Data Protection Act.

- The data controller therefore has both the rights and the obligations to make decisions about the purposes and the means for processing.

- The data controller is responsible for ensuring that there is a legal basis for the processing that the data processor is instructed to perform.

The data processor is acting according to instructions

- The data processor may only process personal data according to documented instructions from the data controller, unless required under EU law or the national law of the Member States to which the data processor is subject; In that case, the data processor shall notify the data controller of this legal requirement before processing unless that court prohibits such notification for reasons of important social interests, cf. Article 28, piece 3, litra a.

- The data processor immediately informs the data controller if an instruction, in the opinion of the data processor, is contrary to the data protection regulation or data protection provisions in other EU law or national law of the Member States.

Confidentiality

- The data processor ensures that only the persons currently authorized to do so have access to the personal data processed on behalf of the data controller. Access to the information must therefore be immediately closed if the authorization is deprived or expired.

- Only persons authorized for access to personal data may be authorized to fulfill the data processor's obligations to the data controller.

- The data processor ensures that the persons authorized to process personal data on behalf of the data controller have committed themselves to confidentiality or are subject to appropriate statutory confidentiality.

- At the request of the data controller, the data processor should be able to demonstrate that the relevant employees are subject to the aforementioned confidentiality obligation.

Security of processing

- The data processor initiates all measures required by Article 32 of the Data Protection Regulation, which among others it is apparent that, taking into account the current level, the implementation costs and the nature, scale, coherence and purpose of the treatment concerned, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons, appropriate technical and organizational measures must be implemented to ensure a level of safety fits these risks.

- The above obligation implies that the data processor must carry out a risk assessment and then take measures to address identified risks. Among other things, the following measures may include, among others, the following:
    - Pseudonymization and encryption of personal data
    - Ability to ensure continued confidentiality, integrity, accessibility and robustness of treatment systems and services
    - Ability to timely restore the availability of and access to personal data in case of a physical or technical incident
    - A procedure for periodic testing, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure treatment safety

- In connection with the above, the data processor must - at least - implement at least the level of security and the measures specified in Appendix C of this Agreement.

- The parties may make any adjustment / agreement on remuneration or the like. In connection with the data controller or data processor's subsequent requirement for establishing additional security measures, it will be apparent from the parties' "main agreement" or from appendix D of this agreement.

Use of sub-data processors

- The data processor must comply with the conditions set out in Article 28 of the Data Protection Regulation. nr 2 and 4, to use another data processor (sub-data processor).

- The data processor may not use another data processor (sub-processor) to fulfill the data processing agreement without prior specific or general written approval from the data controller.

- In the case of general written approval, the data processor must notify the data controller of any planned changes regarding the addition or replacement of other data servers, thereby giving the data controller the opportunity to object to such changes.

- The data controller's terms and conditions for the data processor's use of any sub-data processors are contained in appendix B of this Agreement.

- The data controller's possible authentication of specific sub-data prccesor commuters is listed in Appendix B of this Agreement.

- When the data processor has the data controller's authorization to use a subprocessor, the data processor provides to impose on the data processor the same data protection obligations as those set forth in this data-processing agreement through a contract or other legal document under EU law or national law of the Member States in particular providing the necessary guarantees that the subcontractor will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the Data Protection Regulation.

- The data processor is thus responsible, as far as possible, through the conclusion of a sub-data processor agreement - to impose any subcontractor at least on the obligations that the data processor itself is subject to under the data protection rules and this data processing agreement and its appendices.

- The Data Processing Agreement and any subsequent changes thereto will be sent to the data controller, upon request by the data controller, in order to ensure that a valid agreement has been entered into between the data processor and the subprocessor. Any commercial terms, such as prices that do not affect the data protection content of the Sub-Processing Agreement, should not be sent to the data controller.

- As far as possible, the data processor shall, in his agreement with the sub-processor, insert the data controller as a beneficiary third party in the event of the bankruptcy of the data processor so that the data controller may enter into the data processor's rights and apply them to the sub-data processor, for example. so the data controller can instruct the sub-data processor to delete or retrieve information.

- If the sub-data processor does not comply with its data protection obligations, the data processor remains fully liable to the data controller for the fulfillment of the subcontractor's obligations.

Transfer of information to third countries or international organizations

- The data processor may only process personal data by documented instructions from the data controller, including as regards the transfer (transfer, transfer and internal use) of personal data to third countries or international organizations, unless required under EU law or the national law of the Member States as the data processor is subject to; In that case, the data processor shall notify the data controller of this legal requirement before processing unless that court prohibits such notification for reasons of important social interests, cf. Article 28, piece 3 litra a.

- Without the data controller's instruction or approval, the data processor - within the framework of the data processing agreement - can, among other things, does not;
    - pass personal data to a data controller in a third country or in an international organization,
    - leave the processing of personal data to a sub-data processor in a third country,
    - let the information process in another of the data processor's departments located in a third country.

- The data controller's possible instruction or approval of the transfer of personal data to a third country will appear from Appendix C of this Agreement.

Assistance to the data controller

- The data processor, taking into account the nature of the processing, shall, as far as possible, assist the data controller by appropriate technical and organizational measures, with the obligation of data controller to respond to requests for the exercise of the data subjects' rights as laid down in Chapter 3 of the Data Protection Regulation.

- This implies that, as far as possible, the data processor shall assist the data controller in connection with the data controller being responsible for ensuring compliance with:
    - disclosure obligation for collecting personal data from the data subject

    - disclosure obligation, whose personal data have not been collected by the data subject
    - the registrant's insight
    - right to rectification
    - the right to delete ("the right to be forgotten")
    - the right to limitation of treatment
    - notification obligation in connection with the correction or deletion of personal data or limitation of treatment
    - the right to data portability
    - right of objection
    - the right to object to the result of automatic individual decisions, including profiling

- The data processor assists the data controller in ensuring compliance with the data controller's obligations under Article 32-36 of the Data Protection Regulation, taking account of the nature of the processing and the information available to the data processor, cf. Article 28, piece 3, litra f.

  This implies that, in consideration of the nature of the processing, the data processor shall assist the data controller in ensuring that the data controller is responsible for ensuring compliance with:

    - the obligation to implement appropriate technical and organizational measures to ensure a level of safety appropriate to the risks associated with treatment

    - the obligation to report to the supervisory authority (Data Inspectorate) breach of personal data security without undue delay and, if possible, within 72 hours after the data controller has been notified of the breach unless it is unlikely that the breach of personal data security would endanger the rights of natural persons or freedoms.

    - the obligation - without undue delay - to notify the data subject of personal data breach when such a breach is likely to entail a high risk of the rights and freedoms of natural persons

    - the obligation to carry out an impact assessment on data protection if one type of treatment is likely to pose a high risk to the rights and freedoms of natural persons

    - the obligation to consult the supervisory authority (Data Inspectorate) before processing if an impact assessment on data protection shows that the processing will lead to high risk in the absence of measures taken by the data controller to limit the risk

- Any possible regulation / settlement of the parties or similar in connection with the data processor's assistance to the data controller will appear from the parties' "main agreement" or from Appendix D of this Agreement.

Notification of breach of personal data security

- The Data Processor informs the data controller without undue delay after being aware that there has been a violation of the personal data security of the data processor or any sub-data processor. The data processor's notification to the data controller shall, if possible, be made within 36 hours of the breach of the breach so that the data controller is able to comply with his obligation to report the breach to the supervisory authority within 72 hours.

- In accordance with paragraph 10.2 litra b, of this agreement, the data processor shall - assist in the nature of the processing and the information available to it - assist the data controller in reporting the breach of the supervisory authority. This may mean that the computer shall assist in providing the following information, as provided for in Article 33 piece 3, of the Data Protection Regulation, shall be stated by the data controller's notification to the supervisory authority:

    - The nature of the breach of personal data protection, including, where possible, the categories and the approximate number of registered persons, as well as the categories and the approximate number of personal data records concerned.
    - Probable consequences of the breach of personal data security
    - Measures taken or proposed to address the breach of personal data protection, including where appropriate, measures to limit its possible harmful effects

Deleting and retrieving information

- Upon termination of the processing services, the data processor is obliged to delete or retrieve all personal data to the data controller, as well as to delete existing copies, unless the European Union or national law prescribes the retention of personal data.

Supervision and audit

- The data processor shall make available to the data controller all information necessary for detecting the compliance of the data processor with Article 28 of this Data Protection Regulation and this Agreement, allowing and contributing to audits, including inspections carried out by the data controller or other auditor authorized by the data controller.

- The detailed procedure for the data controller's supervision of the data processor is contained in Appendix C of this agreement.

- The data controller's supervision of any sub-data processor is based on the data processor. The detailed procedure for this is stated in Appendix C of this Agreement.

- The data processor is required to provide authorities with access to the data controller and data processor facilities, or representatives acting on behalf of the Authority, access to the physical facilities of the data processor against duly credentials.

Parties' agreements on other matters

- Any (specific) regulation of the consequences of the parties 'breach of the data processing agreement will be apparent from the parties' "main agreement" or of this Agreement's Appendix D.

- Any regulation of other relationships between the parties will be apparent from the parties' "main agreement" or of this Agreement's Appendix D.

Entry into force and termination

- This Agreement shall enter into force on both parties' signatures.

- The agreement may be renegotiated by both parties if the law changes or inconsistencies in the agreement give rise to this.

- Any adjustment / agreement of the parties regarding remuneration, conditions or the like in connection with changes to this Agreement will appear from the parties' "main agreement" or from Appendix D of this Agreement.

- Termination of the data processing agreement may be in accordance with the termination conditions, including. termination notice, as stated in the "main agreement".

- The agreement is valid for the duration of the treatment. Regardless of the termination of the "Main Agreement" and / or the Data Processing Agreement, the Data Processing Agreement will remain in force until termination of the processing and the deletion of the data by the data processor and any under-processing agents.

- The agreement is concluded electronically and acceptance of the agreement is given by pressing the "Accept" button after reading and accepting this agreement.

Contact persons / contact points of the data controller and data processor

- The parties may contact each other through the registered contact details provided by the electronic acceptance of this data processing agreement.

- The parties are required to continuously inform each other of changes regarding the contact / contact point.

Appendix A - Information on the treatment

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

- The data processor provides the platform for therapists for use in:
    - Client registration
    - Journaling
    - Booking of time / appointment
    - Communication between the therapist and the client

The data processor's processing of personal data on behalf of the data controller is primarily about (the nature of the processing):

The treatment will be done via the Mango Apps' EasyPractice Platform, which is made available to the individual therapist. The platform serves as a system for registering members or clients for the individual therapist. In addition, the system of journalization is used in cases where there are clients who attend a therapist. In the case of clients, it may also be necessary under the Health Act to register the patient's CPR number in relation to eligible treatment.

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

- Email address
- Name
- Social Security No.
- Health information
- Identification for online payment
- Contact information (address, phone number)

The treatment includes the following categories of registrars:

- Persons who have created a free Therapist Profile and / or use the EasyPractice Platform for registration of clients
- People who have created a profile in Secure Messages directly at EasyPractice

The data processor's processing of personal data on behalf of the data controller may commence after the entry into force of this Agreement. The treatment has the following duration:

- The processing is not limited to time and time until the agreement is terminated or terminated by one of the parties

Appendix B - Conditions for the data processor's use of sub-data processor and list of authorized sub-data processor

Conditions for the data processor's use of any sub-data processor
The data processor has the data manager's general authentication to use sub-data processor. However, the data processor must notify the data controller of any planned changes regarding the addition or replacement of other data servers, thereby giving the data controller the opportunity to object to such changes. Such notification shall be the data controller for at least 2 months before the application or amendment is to take effect. If the data controller opposes the changes, the data controller must notify the data processor within 1 month of receiving the notification. The data controller can raise objections only if the data controller has reasonable, concrete reasons for this.

Approved subdatabase
At the entry into force of the data processing contractor, the data controller has approved the use of the following sub-data processor:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
Dinero	34731543	Vesterbrogade 1 L, 6. sal 1620 København V	EasyPractice users can also connect to Dinero and bill their clients through.
Mailgun			Sending og e-mail
Sygeforsikringen Danmark	22656511	Palægade 5, 1261 København K	Reporting of invoices to the health insurance "Denmark"
E-conomic	29403473	Langebrogade 1 1411 København K.	Accounting system used if billing subscription to Therapeut Bookings users. EasyPractice users can also connect to e-conomic and bill their clients through.
MailChimp			EasyPractice users can also connect to MailChimp and manage newsletters to their clients.
Campaign Monitor			We send newsletters to Campaign Monitor to our users.

ePay	28855060	Vandmanden 10 L DK-9200 Aalborg	Processing of payment information.
Stripe			Processing of payment information for the therapist's clients.

At the entry into force of the data processing contractor, the data controller has specifically approved the use of the above sub-data processor for the particular treatment described for the party. The data processor can not, without the data controller's specific and written approval, apply the individual sub-processor to a "second" processing and agree or allow another sub-processor to complete the described processing.

Appendix C - Instructions for processing personal data

The subject of the treatment / instructions
The data processor's processing of personal data on behalf of the data controller is done by the data processor performing the following:

- EasyPractice
  - Sets a system available to the data controller for the creation of clients, booking of appointments, journalization, etc.
- Dinero
  - Exchange of accounting information after specific instructions from the data controller
- Sygeforsikringen Danmark
  - Payment of sickness insurance benefits according to instructions from the data controller
- E-conomic
  - Exchange of accounting information after specific instructions from the data controller
- MailChimp
  - Exchange of email information after specific instructions from the data controller
- Stripe
  - Receiving online payment from clients following specific instructions from the data controller

Security of processing
The security level must reflect:

- The processing of a large amount of common personal data covered by Article 6 of the Data Protection Regulation on "General Personal Data" and, in some cases, also sensitive personal data covered by Article 9 of the Data Protection Regulation, and an "appropriate" level of security should be established accordingly.

The data processor is then entitled and obliged to make decisions about the technical and organizational security measures to be used to create the required (and agreed) security level around the information.

However, the data processor must - in all cases and at least - implement the following measures agreed with the data controller (based on the risk assessment performed by the data controller):

Pseudonymization is used for statistics.

Mango Apps employees are subject to confidentiality and privacy, and these requirements are also part of Mango Apps's personal data policy.
Mango Apps has entered into data processing agreements with sub-data processor including software and systems.

In the event of a physical or technical incident, Mango Apps has the opportunity to restore the availability and access to personal information through back-up in a timely manner.

The effectiveness of the technical and organizational measures to ensure treatment security is tested and tested regularly in collaboration with Mango Apps' sub-processors.

The transfer of personal data to unsafe third countries does not take place and should be applicable, it will be in compliance with the required safeguards for unsafe third countries.

The common personal data are stored in a centralized and protected manner, and data minimization and limitation of access to both common personal data and sensitive personal data has been taken into account.

Physical security of computers and security of access to sites where personal data are processed.

When using home / remote workstation, computers are secured with personal password.

Storage Period / erase routine
The personal data is stored with the data processor until the data controller requests that the information be deleted or returned

Location of treatment
The processing of the personal data contained in the agreement can not be done without the data controller's prior written consent at locations other than the following:

- Mango Apps, Strandlodsvej 44, 3. sal, 2300 København S

Instructions or approvals regarding the transfer of personal data to third countries
Transfer of personal data to a third country will, where appropriate, take place in compliance with the safeguards required under the Data Protection Regulation 5.

Further procedures for the data controller's supervision of the processing performed by the data processor
The data controller or a representative of the data controller also has access to oversight, including physical supervision, at the data processor, when the data controller assesses a need for this.

The data controller's possible expenses in connection with physical supervision shall be borne by the data controller himself. However, the data processor is required to allocate the resources (mainly the time) necessary for the data controller to carry out his supervision.

Further procedures for the supervision of the treatment performed with any sub-data processor

In addition, the data processor or a representative of the data processor has access to oversight, including physical supervision, at the sub-data processor, when a request is made by the data processor (or the data controller).

In addition to the planned supervision, the sub-data processor can be supervised when, after the assessment of the data processor (or the data controller), a need arises.

Documentation for the supervised inspection is sent to the data controller as soon as possible.