Data Processing Agreement

Between

Controller/Data Controller

[name]
[street]
[zip & city]
[vat-number]
Contact person: [mail]

&

Processor/Data Processor

EasyPractice ApS
Vesterbrogade 74, 3.
1620 Copenhagen V, Denmark
VAT number: 35642536
Contact: support@easypractice.net

Content

1. Background for the data processing agreement

1.1. This Data Processing Agreement (“ **Data Processing Agreement** ") sets out the rights and obligations that apply to the processing of personal data by the Data Processor, acting on behalf of the Data Controller.

1.2. The purpose of this Data Processing Agreement is to ensure that the parties comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“the General Data Protection Regulation” or “GDPR”), as well as any applicable laws implementing the GDPR in the jurisdiction where the Data Processor is established (hereinafter collectively referred to as “data protection legislation”).

1.3. The Processor's processing of personal data is carried out for the purpose of fulfilling the main agreement between the parties: "Terms and Conditions" (“ **Main Agreement** "). The processing is described in more detail in Appendix A (Information on the processing).

1.4. In this Data Processing Agreement, "personal data", "Data Controller", "Data Processor", "data subject", "processing", "personal data breach", "supervisory authority", and "third countries" shall be understood in accordance with data protection legislation.

1.5. In the event of any inconsistency between this Data Processing Agreement and the Main Agreement, the Data Processing Agreement shall prevail in all matters concerning the Data Processor's processing of personal data on behalf of the Data Controller.

1.6. This Data Processing Agreement consists of this main body of the agreement and the following appendices: Appendix A (Information on the processing), Appendix B (Sub-processors), and Appendix C (Information Security).

1.7. The Data Processing Agreement and associated documents shall be stored in a written electronic format by both parties.

1.8. The parties agree that the English version of the Data Processing Agreement is the authoritative and official version of this agreement. In case of discrepancies or inconsistencies, the English version shall prevail over translated versions.

1.9. This Data Processing Agreement does not relieve the Data Processor of obligations directly imposed on the Data Processor under data protection legislation.

2. The Controller's rights and obligations

2.1. The Data Controller is responsible for ensuring that the processing of personal data takes place in accordance with data protection legislation.

2.2. The Data Controller has the right and obligation to determine the purpose of the processing of personal data and the means to be used.

2.3. The Data Controller is, among other things, responsible for ensuring that the processing it instructs the Data Processor to carry out is supported by a lawful basis.

3. The Processor acts on instructions

3.1. The Processor may only process personal data in accordance with documented instructions from the Data Controller, unless the Processor is required by EU/EEA law or the law of a Member State to which the Processor is subject to process personal data in another way. If such a legal obligation arises, the Processor shall inform the Data Controller of the legal requirement before processing, unless that law prohibits such notification on important grounds of public interest, cf. Article 28(3)(a).

3.2. The Processor shall immediately inform the Data Controller if the Processor believes that an instruction from the Data Controller infringes data protection legislation.

4. Confidentiality

4.1. The Processor shall ensure that access to the personal data processed on behalf of the Data Controller is limited to persons authorized to have such access.

4.2. The Processor shall ensure that persons authorized to process personal data on behalf of the Data Controller are subject to a statutory or contractual duty of confidentiality.

4.3. Upon request from the Data Controller, the Processor shall be able to demonstrate that employees and other persons authorized to process personal data on behalf of the Data Controller are subject to a duty of confidentiality.

5. Security of processing

5.1. The Processor shall implement all measures required under Article 32 of the GDPR. This means that the Processor shall, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing personal data.

5.2. The above obligation implies that the Processor must carry out a risk assessment and then take measures to address identified risks. Such measures may include, *inter alia*, the following:

5.2.1. Pseudonymization and encryption of personal data;

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

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

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

5.3. The relevant measures are specified in Appendix C (Information Security). The Data Controller must provide the Data Processor with all necessary information to identify and assess such risks. In connection with the Data Controller's or Data Processor's subsequent need for implementing additional security measures, such additional measures must be specified in the main agreement or in Appendix C (Information Security).

6. Use of sub-processors

6.1. The Processor shall comply with the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation in order to engage another Processor for carrying out specific processing activities on behalf of the Data Controller ("sub-processor").

6.2. The Processor shall not use a sub-processor to process personal data under this Data Processing Agreement without the Data Controller's prior written consent.

6.3. The Data Controller hereby gives the Processor its general authorization to use sub-processors to fulfill the Data Processing Agreement. Sub-processors in use at the time of entering into this Data Processing Agreement are listed in Appendix B (Sub-processors).

6.4. In the event of replacement of one or more of the sub-processors mentioned in Appendix B (Sub-processors), or appointment of new sub-processors, the Processor shall inform the Data Controller within a reasonable time before the

new sub-processor is used. The Data Controller may object to such changes if there are reasonable grounds to believe that the engagement will reduce the level of protection guaranteed for the personal data under this Data Processing Agreement. If the Data Controller objects to the use of the sub-processor, the parties shall in good faith enter into discussions with the aim of finding a solution that addresses the Data Controller's concerns.

6.5. When the Processor engages a sub-processor in accordance with this Section 6, the Processor shall ensure that the sub-processor is bound by the same obligations as those imposed on the Processor under this Data Processing Agreement.

6.6. The Processor's use of sub-processors shall not reduce or limit the Processor's liability and obligations under this Data Processing Agreement.

7. Transfers to third countries or international organizations

7.1. The Processor shall not, without the Data Controller's prior written consent, transfer or otherwise cause personal data to be transferred outside the EU/EEA area to third countries or international organizations not recognized by the European Commission as providing an adequate level of protection for personal data. Before such consent is given, the Data Controller may require the Processor to take appropriate safeguards, including (but not limited to) ensuring that the transfer takes place on the basis of the EU Commission's standard contractual clauses for the transfer of personal data to third countries.

8. Assistance to the controller

8.1. The Processor shall, by means of appropriate technical and organizational measures, assist the Data Controller in responding to requests from data subjects regarding the exercise of the data subject's rights vis-à-vis the Data Controller under Chapter III of the GDPR.

8.2. Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations under Articles 32-36 of the GDPR. This means that the Processor shall assist the Data Controller in ensuring compliance with:

8.2.1. The obligation to carry out a data protection impact assessment, if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons (“ **data protection impact assessment** " or “ **DPIA** “).

8.2.2. The obligation to consult the supervisory authority (Datatilsynet) before processing, if a DPIA indicates that the processing would result in a high risk in the absence of measures to mitigate the risk.

8.3. The Processor is entitled to compensation for time spent assisting the Data Controller, if this has been agreed in the main agreement or in Appendix C (Information Security).

9. Personal data breach

9.1. The Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach at the Processor or a sub-processor. The Processor shall provide the necessary information and assistance to enable the Data Controller to fulfil its notification obligations under data protection legislation. The Processor shall furthermore take all the required measures to limit the impact of the personal data breach.

10. Deletion and return of data

10.1. Upon termination of the Data Processing Agreement, the Data Controller may, if possible, instruct the Processor to return all personal data processed by the Processor on behalf of the Data Controller to the Data Controller or to a third party designated by the Data Controller. The Data Controller may also request the deletion of the personal data. The Processor shall, within a reasonable time after receiving such an instruction, send written confirmation that the personal data has been returned and/or deleted.

11. Access and audit

11.1. The Processor shall make available to the Data Controller all information necessary to demonstrate the Processor's compliance with Article 28 of the GDPR and this Data Processing Agreement. The Processor shall enable and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller, to verify that the Processor complies with its obligations under this Data Processing Agreement.

11.2. The detailed procedure for the Data Controller's supervision of the Data Processor is described in Appendix C (Information Security).

11.3. The Data Controller's supervision of any sub-processors shall be carried out via the Data Processor. The detailed procedure for this is described in Appendix C (Information Security).

12. Liability

12.1. The limitation of liability stated in the Main Agreement shall apply equally to any breach of this Data Processing Agreement committed by a party.

12.2. The parties' liability for damages suffered by data subjects or other natural persons as a result of infringements of data protection legislation is subject to Article 82 of the GDPR, without the above limitation being covered by this.

13. Entry into force and termination

13.1. This Data Processing Agreement shall enter into force on the date of signature of this Data Processing Agreement by both parties.

13.2. Each party may request renegotiation of the Data Processing Agreement if changes in legislation or deficiencies in the Data Processing Agreement provide grounds for doing so.

13.3. Any subsequent changes regarding remuneration, terms, or similar matters will be specified in the main agreement or in Appendix C (Information Security).

13.4. The Data Processing Agreement may be terminated in accordance with the provisions of the Main Agreement.

13.5. The Data Processing Agreement shall remain in effect as long as the Data Processor processes personal data on behalf of the Data Controller. Notwithstanding the termination of the Main Agreement, the Data Processing Agreement shall remain in effect until the processing ceases and the personal data is deleted by the Data Processor and any involved sub-processors.

14. Notices

14.1. Notices, communications, or other forms of communication between the Data Controller and the Data Processor, which must be given in writing according to this Data Processing Agreement, shall be sent via e-mail as specified in Appendix A (Information on the processing).

15. Applicable law and jurisdiction

15.1. The provisions of the Main Agreement on choice of law and jurisdiction shall apply mutatis mutandis to this Data Processing Agreement.

Appendix A - Information on the processing

1. Purpose of processing - The Processor's processing of personal data on behalf of the Data Controller is for the purpose of providing access to and use of the EasyPractice platform, including: - Client management - Record keeping - Booking of appointments/online courses/events - Communication between therapists and patients - Invoicing and payment

2. Nature of processing - The processing takes place via the EasyPractice platform used by the Data Controller. This includes storage and administration of client and patient records, booking information, communication, and invoicing data.

3. Duration of processing **-** The processing continues as long as the Main Agreement between the parties is valid, and until all personal data has been deleted or returned to the Data Controller in accordance with this Data Processing Agreement.

4. Categories of data subjects - The Data Controller's employees who use the platform - The Data Controller's clients/patients who book appointments or interact via the platform

5. Types of personal data - Name - Email - Contact information (address, phone number) - SSN number (where legally required) - Health data (as a special category of data) - User ID assigned by the system - Payment IDs (e.g., invoice number, transaction ID)

6. Special categories of data - Health data in accordance with Article 9 of the GDPR.

7. Use of sub-processors may only be used for the purposes necessary to provide the services described in this Appendix A. All sub-processors must process data in strict accordance with the Data Controller's instructions and only to perform their designated functions.

- Provide the platform to the controller. The platform includes the following features for end users:
    - Client management
    - Record keeping
    - Booking of appointments/online courses/events
    - Communication between therapists and
    - Invoicing and payment

The Processor's processing of personal data on behalf of the Data Controller primarily concerns (nature of processing):

The processing will take place via the platform (“ **the System** ") made available to the individual therapist. The platform functions as a system for registering members or clients of the individual therapist. In addition, the system is used for record keeping in cases where clients visit a therapist. In relation to clients, it may also be necessary, in accordance with health legislation, to register the patient's SSN number in connection with service-eligible treatment.

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

- E-mail
- Name
- SSN number
- Identification for online payment
- Contact information (address, phone number)
- User ID number issued by the system

The processing includes the following categories of data subjects:

- The customer and the customer's employees who have created a profile and/or use the system for client registration.
- The customer's customers who have created a profile in Online Booking directly through the system.

Special categories of personal data:

- Health data

Appendix B - Sub-processors

By entering into this Data Processing Agreement, the Data Controller has approved the use of the following sub-processors:

Name	**Nature and purpose of processing**	**Categories of personal data**	**Location**
Wannafind	Cloud hosting provider	All personal data - our databases and servers are hosted here.	https://www.wannafind.dk/, Denmark
Amazon Web Services	Cloud hosting and technical service provider, processing backups	All personal data.	EU regions only
Google	Technical service provider - maps, analytics, calendar features	IP address used in analytics (only if enabled by user); Google Calendar sends client names (only if enabled by user).	https://analytics.google.com/, https://calendar.google.com/, United States
Intercom, Inc.	Cloud-based in-app support chat platform	All personal data - our customers may share any data in support requests.	Ireland
Mailgun Technologies Inc.	Email delivery service.	Email addresses, message content.	United States
MailChimp	Email marketing and automation platform.	Email addresses, subscriber data, campaign data (only if enabled by user).	United States
Cpsms	SMS messaging service.	Phone numbers, message content.	Denmark
SMS DK	SMS messaging service.	Phone numbers, message content.	Denmark

Stripe	Processing online payments and subscriptions.	Payment card details, billing address, transaction history.	United States and EU
Posthog	Product analytics platform	User events, website interactions (only anonymized user IDs and no PII are shared).	United States and EU
MixPanel	Product analytics platform	User events, website interactions, and potentially other user data.	United States
ChartMogul	Subscription analytics platform.	Subscription data, revenue information, and customer data.	United States
Hubspot, Inc.	Marketing automation and CRM platform.	User contact information, marketing data, and customer data.	Germany
HotJar	Website analytics and user feedback.	Website visitor behavior, feedback data (e.g., surveys, heatmaps).	EU
Onpay	Payment gateway.	Payment data, transaction details.	Denmark
Dinero	Financial accounting app	Financial data, invoicing data, and customer data (only if enabled by user).	Denmark
Economic	Financial accounting app	Financial data, invoicing data, and customer data (only if enabled by user).	Denmark

Fiken	Financial accounting app	Financial data, invoicing data, and customer data (only if enabled by user).	Norway
Fortnox	Financial accounting app	Financial data, invoicing data, and customer data (only if enabled by user).	Sweden
Helsenett	Digital services for healthcare professionals	Patient data, medical records, and other sensitive health information (only if enabled by user).	Norway
Zapier	Automation service provider	Data from connected apps, which could include user data (only if enabled by user).	United States
Altcha	Cloud based SMS spam detection service	User interaction data for bot detection.	EU
Billy	Financial accounting app	Financial data, invoicing data, and customer data (only if enabled by user).	Denmark
Danmark	Health insurance service	Insurance-related data, claims data, policyholder data (only if enabled by user).	Denmark
Helfo	Health insurance service	Patient data, health service data, and financial data related to health services (only if enabled by user).	Norway

Criipto	Digital identity and signing.	User identity data, signing data.	Denmark
Netsuite	Enterprise resource planning software	Various business data, which may include customer data, financial data, etc.	United States
Facebook	Social authentication solution and analytics service	Public Facebook profile information (only if enabled by user).	United States
Cloudflare	Domain management service	Website visitor data, IP addresses, security logs.	United States
Mobilepay	Payment solution	Payment data, transaction details, user information (only if enabled by user).	Denmark
Epay	Payment solution	Payment data, transaction details.	Denmark
Vipps	Payment solution	Payment data, transaction details, user information (only if enabled by user).	Norway
Zettle	Mobile point of sale (mPOS) system.	Transaction data, payment information (only if enabled by user).	Sweden
New Relic	Performance monitoring and observability.	Application performance data, which may include some user data.	United States

Notion	Team collaboration and documentation software	User-generated content, which may include personal data.	United States
Pusher	Real time communication software	Data related to real-time events and messages, which may include user data.	United Kingdom
What is my browser	Service for identifying browser information.	Browser type, version, and other technical details.	N/A (Location not specified in source)
IpApi	Geolocation by IP address lookup service	IP addresses.	United States
Geoplugin	Geolocation by IP address lookup service	OP addresses.	N/A (Location not specified in source)
Bing	Analytics service, used for tracking conversions	Search queries, user behavior on Bing.	United States
Sentry	Error monitoring and reporting software	Error logs, which may contain some user data.	United States
Speechmatics	Real-time speech to text transcription software	Audio data, transcripts.	United Kingdom
Campaign Monitor	Email marketing platform	Email addresses, subscriber data, campaign data.	United States
Tryg Behandlerbooking	Online booking platform for therapists.	Therapist data, client data, appointment data, and communication between therapists and clients (only if enabled by user).	Denmark

Digicare	Digital solutions for healthcare.	Patient data, medical records, communication data between patients and healthcare providers, and appointment data (only if enabled by user).	Norway
Exorlive	Digital exercise and training platform.	User exercise data, health data (only if enabled by user).	Norway
Medcom	Danish healthcare communication network.	Patient data, medical records, and other sensitive health information (only if enabled by user).	Denmark
KMD	Provides data transmission services (VANS protocol) for Medcom data.	Patient data, medical records, and other sensitive health information related to Medcom (only if enabled by user).	Denmark

Note: Any new sub-processors will be notified to the Data Controller in advance, allowing for objections. Sub-processors may only process data for the purposes described in Appendix A.

Appendix C - Information Security

1. Security Measures - The Data Processor shall implement the following technical and organizational measures in accordance with Article 32 of the GDPR:

a. Processing security - Secure user authentication (e.g., 2FA) - Role-based access controls - TLS encryption in transit, AES-256 encryption at rest - Regular vulnerability scanning and penetration testing

b. Risk assessment - Annual internal and external risk assessments - Continuous monitoring of risk exposure

c. Antivirus and firewall - Enterprise-grade firewall systems - Up-to-date antivirus software on all endpoints

d. IP locking and certificates - HTTPS with valid SSL certificates

e. User and administrator access - Principle of least privilege - Onboarding/offboarding access procedures

f. Monitoring and logging - System activity logs with audit trails - Real-time alerts for suspicious behavior

g. Organizational measures - Internal data protection policies - Annual GDPR and security training for all employees

h. Secure communication - Encrypted communication channels (HTTPS, TLS) - Secure messaging systems

i. Encryption - Encryption of personal data both in transit and in storage - Encryption keys managed and rotated securely

j. Backup - Daily encrypted backups stored in EU data centers - Regular testing of backup and recovery

k. Physical security - Secured data centers with 24/7 monitoring

l. Employee security - Confidentiality agreements signed by all employees - Access limited to authorized personnel

m. Other measures - Incident response plan in place

2. Instructions - The Processor may only process personal data based on the documented instructions from the Data Controller as defined in this Data Processing Agreement and any further written instructions issued during the term of the agreement.

3. Retention and deletion routine - Data is stored for the duration of the agreement. Upon termination or at the Data Controller's request: - Data is deleted within 30 days - Written confirmation of deletion is provided - Secure deletion procedures are applied to all media

4. Processing location - All data is processed and stored within the EU/EEA. No data is transferred to third countries without prior written consent from the Data Controller.

5. Transfers to third countries - No transfers of personal data to third countries shall take place unless otherwise agreed in writing with the Data Controller. If such transfers are made, appropriate safeguards (e.g., standard contractual clauses) will be implemented.

6. Audit and control - The Processor conducts an annual internal audit of its data processing and information security controls. The results are documented and available to the Data Controller upon request. The Processor also allows the Data Controller to conduct its own audit or designate a third party (who must not be the Processor's competitor) to perform an audit with reasonable notice and during normal business hours.

7. Bankruptcy / Third-party beneficiary - In case of the Processor's bankruptcy the Data Controller (or a designated third party) shall have access to retrieve personal data and backups to ensure continuity and protection of data subjects' rights.

The level of security must reflect:

- Processing of a large amount of ordinary personal data as covered by Article 6 of the GDPR, and in some cases also sensitive personal data as covered by Article 9 of the GDPR. Accordingly, an "appropriate" level of security must be established.

The Data Processor then has the right and obligation to decide on the technical and organizational security measures to be applied to ensure the necessary (and agreed) level of data security.

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 carried out by the Data Controller):

Pseudonymization is used for statistics.