Data Processing Agreement

Between

**Controller**

Customer

&

**Processor**

EasyPractice ApS
Strandlodsvej 44, 3. sal
2300 København S Denmark
CVR 35642536
Kontakt: support@easypractice.net

# Contents

[**Contents 2**](#_3znysh7)

[**1. Background for the Data Processing Agreement 3**](#_tyjcwt)

[**2. Rights and obligations of the controller 3**](#_3dy6vkm)

[**3. The processor acts on instructions 4**](#_1t3h5sf)

[**4. Confidentiality 4**](#_4d34og8)

[**5. Security of processing 4**](#_2s8eyo1)

[**6. Use of sub-processors 5**](#_17dp8vu)

[**7. Transfers to third countries or international organisations 6**](#_3rdcrjn)

[**8. Assistance to the controller 6**](#_26in1rg)

[**9. Personal data breach 7**](#_lnxbz9)

[**10. Deletion and return of data 7**](#_35nkun2)

[**11. Access and audit 7**](#_1ksv4uv)

[**12. Liability 8**](#_44sinio)

[**13. Entry into force and termination 8**](#_2jxsxqh)

[**14. Notices 8**](#_z337ya)

[**15. Governing law and legal venue 8**](#_3j2qqm3)

[**Appendix A - Information about the processing 9**](#_1y810tw)

[**Appendix B - Sub-processors 10**](#_4i7ojhp)

[**Appendix C - Information Security 11**](#_2xcytpi)

#

# Background for the Data Processing Agreement

* 1. This data processing agreement (the "**Data Processing Agreement**") sets out the rights and obligations governing the processing of personal data by the processor, acting on behalf of the controller.
	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 the "**GDPR**"),and applicable Norwegian law implementing the General Data Protection Regulation (hereinafter collectively referred to as the "**Data Protection Legislation**").
	3. The processor's processing of personal data is carried out in order to execute the main agreement between the parties: "Terms and conditions" (the "**Main Agreement**"). The processing is described in more detail in Appendix A (Information about the processing).
	4. In this Data Processing Agreement, "personal data", "controller", "processor", "data subject", "processing", "personal data breach", "supervisory authority" and "third countries" shall be understood in accordance with the Data Protection Legislation.
	5. In case of conflict between this Data Processing Agreement and the Main Agreement, the Data Processing Agreement shall take precedence regarding all matters concerning the processor's processing of personal data on behalf of the controller.
	6. This Data Processing Agreement consists of this main body of the agreement and the following appendices: Appendix A (Information about the processing), Appendix B (Sub-processors) and Appendix C (Information Security).
	7. The Data Processing Agreement and associated documents are kept in a written electronic format by both parties.
	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 any discrepancies or inconsistencies, the English version shall take precedence over any translated versions.
	9. This Data Processing Agreement shall not relieve the processor of any obligations that are imposed directly on the processor under Data Protection Legislation.

# Rights and obligations of the controller

* 1. The controller is responsible for ensuring that the processing of personal data is carried out in accordance with the Data Protection Legislation.
	2. The controller has the right and duty to determine the purpose of the processing of personal data and the means to be employed.
	3. The controller is responsible for, among other things, ensuring that the processing which it instructs the processor to perform is supported by a lawful basis.

# The processor acts on instructions

* 1. The processor may only process personal data in accordance with documented instructions from the controller, unless the processor is obliged pursuant to EU/EEA law or Member State law to which the processor is subject to process personal data in a different manner. If such legal obligation arises, the processor shall inform the controller of the legal requirement before processing, unless that law prohibits such notification on important grounds of public interests, cf. Article 28(3)(a).
	2. The processor shall immediately inform the controller if the processor is of the opinion that an instruction from the controller infringes Data Protection Legislation.

# Confidentiality

* 1. The processor shall ensure that access to the personal data processed on behalf of the controller is restricted to individuals who are authorised to have such access.
	2. The processor shall ensure that the persons authorised to process personal data on behalf of the controller are subject to a statutory or contractual duty of confidentiality.
	3. At the request of the controller, the processor shall be able to demonstrate that employees and other persons authorised to process personal data on behalf of the controller are subject to a duty of confidentiality.

# Security of processing

* 1. The processor shall implement all measures required under Article 32 of the GDPR. This means that the processor shall implement, taking into account the technological development, the costs of implementation and the nature, scope, context and purpose of the processing in question, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, appropriate technical and organisational measures to ensure an adequate level of security for the processing of personal data.
	2. The above obligation implies that the processor must carry out a risk assessment and thereafter take measures to manage identified risks. Such measures may include, *inter alia*, the following:
		1. Pseudonymisation and encryption of personal data;
		2. measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services;
		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
		4. a process for regularly testing, analysing and assessing the effectiveness of the technical and organisational measures of the processing.
	3. The relevant measures are specified in Annex C (Information Security). The controller shall provide the processor with all information necessary to identify and assess such risks. In connection with any subsequent need of the controller or processor for the implementation of additional security measures, such additional measures shall be specified in the main agreement or in Appendix C (Information Security).

# Use of sub-processors

* 1. The processor shall comply with the terms of Article 28 (2) and (4) of the General Data Protection Regulation in order to engage another processor for processing contemplated by this Data Processing Agreement ("**sub-processor**").
	2. The processor may not use a sub-processor to process personal data under this Data Processing Agreement without the prior written consent of the controller.
	3. The controller hereby grants the processor its general authorisation to use sub-processors to perform the Data Processing Agreement. Sub-processors that are in use at the time of conclusion of this Data Processing Agreement are specified in Appendix B (Sub-processors).
	4. In the event of a replacement of one or more of the sub-processors mentioned in Appendix B (Sub-processors), or the appointment of new sub-processors, the processor shall notify the controller within a reasonable time prior to using the new sub-processor. The 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 controller objects to the use of the sub-processor, the parties shall, in good faith, initiate discussions with the aim of finding a solution that addresses the concerns of the controller.
	5. When the processor engages a sub-processor in accordance with this clause 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. The processor's use of sub-processors shall not reduce or limit the processor's responsibilities and obligations under this Data Processing Agreement.

# Transfers to third countries or international organisations

* 1. The processor shall not, without the controller's prior written consent, transfer or otherwise cause the personal data to be transferred outside the EU/EEA area to third countries or international organisations that are not recognized by the European Commission as countries ensuring an adequate level of protection for personal data. Before such consent is given, the controller may require the processor to take appropriate safeguards, including (but not limited to) ensuring that the transfer occurs on the basis of the EU Commission's standard contractual clauses for transfers of personal data to third countries.

# Assistance to the controller

* 1. The processor shall, by means of appropriate technical and organisational measures, assist the controller in responding to requests from data subjects concerning the exercise of the data subject's rights vis-à-vis the controller pursuant to Chapter III of the GDPR.
	2. Taking into account the nature of the processing and the information available to the processor, the processor shall assist the controller in ensuring compliance with the controller's obligations pursuant to Articles 32-36 of the GDPR. This means that the processor shall assist the controller in ensuring compliance with:
		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**").
		2. the obligation to consult with the supervisory authority (Datatilsynet) before processing if a DPIA indicates that the processing will result in a high risk if the controller does not implement measures to mitigate the risk.
	3. The processor is entitled to compensation for time spent for assistance to the controller if this is agreed in the main agreement or in Appendix C (Information Security).

# Personal data breach

* 1. The processor shall inform the 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 controller to fulfill its notification obligations pursuant to Data Protection Legislation. The processor shall further take all necessary measures to limit the impact of the personal data breach.

# Deletion and return of data

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

# Access and audit

* 1. The processor shall make available to the 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, that are carried out by the controller or another auditor authorised by the controller to verify that the processor is complying with its obligations under this Data Processor Agreement.
	2. The detailed procedure for the controller's supervision of the processor is set out in Appendix C (Information security).
	3. The controller's supervision of any sub-processors is carried out via the processor. The detailed procedure for this is set out in Annex C (Information Security).

# Liability

* 1. The limitation of liability stated in the Main Agreement equally applies to any breach by a party of this Data Processing Agreement.
	2. The liability of the parties for the losses suffered by data subjects or other natural persons due to breaches of the Data Protection Legislation shall be governed by Article 82 of the GDPR, without being subject to the above limitation.

# Entry into force and termination

* 1. This Data Processing Agreement becomes effective on the date of both parties' signature of the Main Agreement.
	2. Each party may request the Data Processing Agreement to be renegotiated if changes in the law or inadequacies in the Data Processing Agreement provide grounds for doing so.
	3. Any subsequent changes related to remuneration, terms or similar matters will be set out in the main agreement or in Appendix C (Information Security).
	4. The Data Processing Agreement may be terminated in accordance with the provisions of the Main Agreement.
	5. The Data Processing Agreement remains effective as long as the processor processes personal data on behalf of the controller. Regardless of the termination of the Main Agreement, the Data Processing Agreement will remain in force until the processing is terminated and the personal data is deleted by the Processor and any sub-processors involved.
	6. The Data Processing Agreement is entered into electronically, and acceptance of the agreement is confirmed by pressing the "accept" button after reading and agreeing to the terms of this agreement.

# Notices

* 1. Announcements, notifications or other forms of communication between the controller and the processor, which are to be provided in writing as per this Data Processing Agreement, shall be sent by e-mail as specified in Appendix A (Information about the processing).

# Governing law and legal venue

* 1. The provisions of the Main Agreement on choice of law and legal venue shall apply correspondingly to this Data Processing Agreement.

# Appendix A - Information about the processing

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

* 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 terapeuts and patients
	+ Invoicing and payment

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

The processing will take place through the platform (the **"System**") 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 for record keeping is used in cases where there are clients who go to a therapist.

In relation to clients, it may also be necessary, in accordance with the healthcare legislation, to register the patient's social security number in connection with treatment eligible for benefits.

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

* Email
* Name
* Social security number
* Identification for online payment purposes
* Contact information (address, telephone number)
* User ID number issued by the System

**The processing includes the following categories of data subjects:**

* The Customer and employees of the Customer who have created a profile and/or use the System for client registration.
* The clients of the Customer 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 the Data Processing Agreement, the controller has approved the use of the following sub-processors: [Sub Data Processors](https://docs.google.com/spreadsheets/d/1QbAFma7w_KatGQPkE3p4WgSKZpSkOatfAiDfMecAMvc)

# Appendix C - Information Security

**Information Security**

The level of security shall reflect:

* The 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. An "appropriate" level of security must be established accordingly.

The processor then has the right and duty to make decisions about the technical and organisational security measures to be employed to ensure the necessary (and agreed) level of security for the data.

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

Pseudonymisation is employed for statistics.