speedio.

Data Processing Agreement

CUSTOMER LOCATED WITHIN EU

(the "Data Controller")

AND

SPEEDIO APS
FUGLSANGVEJ 97
8500, GRENÅ
DENMARK
CVR: DK-38158724

(the "Data Processor")

Table of contents

1 Data processing agreement

1.1. The *Agreement* is regarding the new EU regulations that states how data should be stored, managed and retained for a certain time, along with procedures for datamanipulation. This agreement is regarding the *Data Processor* processing of personal data on behalf of the *Data Controller*.

1.2. This *Agreement* has been concluded with the *Data Controller* use of the *Data Controller* services as part of the subscription and additional services described in *Speedio ApS* main agreement.

1.3. *Data Processing Agreement* and the Master Agreement shall be interdependent and cannot be terminated separately. The *Data Processing Agreement* may however without termination of the Master Agreement be replaced by an alternative valid data processing agreement.

1.4. This *Data Processing Agreement* shall take priority over any similar provisions contained in other agreements between the *Parties*, including the Master Agreement.

2 Purpose

2.1. The *Data Processor* may only interact with the personal data if necessary to fulfil the obligations of the *Data Processor* and to provide the service agreed upon in the *Main Agreement*.

3 Obligations of the Data Controller

3.1. The *Data Controller* warrants that personal data is proccessed only for legitimate purposes and that the *Data Processor* is not processing more data than required to fulfilling the obligations.

3.2. The *Data Controller* therefore have both the right and obligation to make decisions about the purposes and means of the processing of personal data and are responsible for ensuring that the processing that the *Data Processor* is instructed to perform is authorised in law.

4 Obligations of the Data Processor

4.1. The *Data Processor* may only process the data provided by the *Data Controller* when documented instructions are delivered by the *Data Controller*.

If European Union law or law of a EU Member State demands the *Data Processor* to process the data, the *Data Processor* are required to follow these instructions. In this case, the *Data Processor* must inform the *Data Controller* of the demand before processing the instruction if not prohibited by the legislation.

Does an instruction from the *Data Controller* infringes the EU General Data Protection Regulation or the data protection provisions of a EU Member State in the *Data Processor* opinion, the *Data Processor* must inform the *Data Controller* about this immediately.

4.2. The *Data Processor* must take all necessary precaution to secure the data provided by the *Data Controller*. This to ensure that the data is not accidentally or unlawfully destroyed, lost, brought to the knowledge of unauthorised third parties, abused or processed in any other manner which is contratry to the Danish data protection legislation.

4.3. The *Data Processor* must ensure that any employee processing the data are authorized or are under the appropriate statutory obligation of confidentiality.

4.4. Does the *Data Controller* request documents of how the *Data Processor* complies with the requirements of the applicable data protection legislation, including how the procedures and data flow for the *Data Processor* works within, the *Data Processor* must reply with documents explaining this.

4.5. The *Data Processor* must, as far as possible, assist the *Data Controller*, with appropriate technical and organisational measures, to respond to any request for exercising the data subject's rights.

4.6. If a data subject is requestet then the *Data Processor* must forward this to the *Data Controller* for further processing. In case if the *Data Processor* is entitled to handle such a request, the *Data Processor* can do so.

4.7. If the *Data Processor* processes data in another EU member state, the *Data Processor* must comply with the legislations concerning security measures for that member state.

5 Confidentiality

5.1. The *Data Processor* shall ensure that only those persons who are currently authorised to do so are able to access the personal data being processed on behalf of the *Data Controller*. Access to the data shall therefore without delay be denied if such authorisation is removed or expires.

5.2. Only persons who require access to the personal data in order to fulfil the obligations of the *Data Processor* to the *Data Controller* shall be provided with authorisation.

5.3. The *Data Processor* shall ensure that persons authorised to process personal data on behalf of the *Data Controller* have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

6 Security of processing

6.1. The *Data Processor* shall ensure the confidentiality, integrity and availability of personal data. The *Data Processor* shall implement systematic procedures and technical measures to insure an appropriate level of security, taking into consideration the state and consideration of the implementation in relation to the likelihood and risk of the processing.

6.2. The *Data Processor* shall maintain an high level of security in its services and product, specially where personal data is present. This security is provided through technical, organisational and physical security measures which include:

(6.2.1) Offices and location facilities are protected by appropriate access controls that ensure only authorised access.

(6.2.2) Logging of staff are in place where its appropriate.

(6.2.3) Antivirus, malware checker, rootkit detected is installed and updated frequently.

(6.2.4) Serveraccess is only allowed to certain staff members.

(6.2.5) Staff have rollbased access, and do therefore not have access to anything that they dont need.

(6.2.6) Encrypted connection is used anywhere, if possible.

(6.2.7) Communication between staff members is encryptet.

The *Data Processor* is updating security measures in tact with upcomming threats, and the *Data Processor* is justified to make further decisions on implementing technical and organisational security measures to maintain and safe security level.

7 Retention period

7.1. Personal data that is stored in our system are deleted or anonymised within a reasonable time after the *Data Controller* has completly terminated the Main Agreement which includes products and services. Data which is legally required to store by the *Data Processor* and can therefore be stored in regulation to the legally reguirements.

8 Physical location of data

8.1. Personal data is hosted servers in Roubaix France, Denmark along with Falkenstein and Nuremberg Deutschland. The *Data Controller* hereby authorises the *Data Processor* to move data to one or several other servers located within the European Union if the *Data Processor* finds this relevant and the same level of security can be ensured.

9 Use of sub-processors

9.1. The *Data Processor* shall meet the requirements specified in Article 28, sub-section 2 and 4, of the General Data Protection Regulation in order to engage another processor (Sub-Processor).

9.2. The *Data Processor* shall therefore not engage another processor (Sub-Processor) for the fulfilment of this *Data Processing Agreement* without the prior specific or general written consent of the *Data Controller*.

9.3. In the event of general written consent, the *Data Processor* shall inform the *Data Controller* of any planned changes with regard to additions to or replacement of other *Data Processor*'s and thereby give the *Data Controller* the opportunity to object to such changes.

9.4. When the *Data Processor* has the *Data Controller* s authorisation to use a sub-processor, the *Data Processor* shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this *Data Processing Agreement* on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

The *Data Processor* shall therefore be responsible on the basis of a sub-processor agreement for requiring that the sub-processor at least comply with the obligations to which the *Data Processor* is subject pursuant to the requirements of the General Data Protection Regulation and this *Data Processing Agreement*.

9.5. A copy of such a sub-processor agreement and subsequent amendments shall at the *Data Controller* s request be submitted to the *Data Controller* who will thereby have the opportunity to ensure that a valid agreement has been entered into between the *Data Processor* and the Sub-Processor. Commercial terms and conditions, such as pricing, that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the *Data Controller*.

9.6. The *Data Processor* shall in his agreement with the Sub-Processor include the *Data Controller* as a third party in the event of the bankruptcy of the *Data Processor* to enable the *Data Controller* to assume the *Data Processor* s rights and invoke these as regards the Sub-Processor, e.g. so that the *Data Controller* is able to instruct the Sub-Processor to perform the erasure or return of data.

9.7. The *Data Controller* hereby grants the *Data Processor* a general permission to enter standard contracts with sub-Data Processors outside the EU/EEA on behalf of the *Data Controller*.

9.8. If the Sub-Processor does not fulfil his data protection obligations, the *Data Processor* shall remain fully liable to the *Data Controller* as regards the fulfilment of the obligations of the Sub-Processor.

10 Notification of personal data breach

10.1. On discovery of personal data breach at the *Data Processor* s facilities or a sub-processors facilities, the *Data Processor* shall without undue delay notify the *Data Controller*. The *Data Processor* s notification to the *Data Controller* shall, if possible, take place within 48 after the *Data Processor* has discovered the breach to enable the *Data Controller* to comply with his obligation, if applicable, to report the breach to the supervisory authority within 72 hours.

10.2. According to Clause 9.2., para b, of this *Data Processing Agreement*, the *Data Processor* shall taking into account the nature of the processing and the data available assist the *Data Controller* in the reporting of the breach to the supervisory authority.

This may mean that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33, sub-section 3, of the General Data Protection Regulation, shall be stated in the Data Controllers report to the supervisory authority:

(10.2.1) The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records

(10.2.2) Probable consequences of a personal data breach

(10.2.3) Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage

11 Transfer of data to sub-Data Processors or third parties

11.1. The *Data Processor* shall solely be permitted to process personal data on documented instructions from the *Data Controller*, including as regards transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or Member State law to which the *Data Processor* is subject; in such a case, the *Data Processor* shall inform the *Data Controller* of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.

11.2. Without the instructions or approval of the *Data Controller*, the *Data Processor* therefore cannot within the framework of this *Data Processing Agreement*:

(11.2.1) Disclose personal data to a *Data Controller* in a third country or in an international organisation

(11.2.2) Assign the processing of personal data to a sub-processor in a third country

(11.2.3) Have the data processed in another of the *Data Processor* s divisions which is located in a third country

12 Inspection of Data Processor

12.1. The *Data Processor* shall make available to the *Data Controller* all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement, and allow for and contribute to audits, including inspections performed by the *Data Controller* or another auditor mandated by the *Data Controller*.

12.2. Additional to the above, the *Data Processor* must assist the *Data Controller* in ensuring compliance with the Data Controllers obligations under article 32-36 of the General Data Protection Regulation.

12.3. Any requests to the *Data Processor* can be charged with an hourly rate of 350 DKK.

13 Commencement and termination

13.1. This *Data Processing Agreement* shall become effective on the date of both Parties signature to this *Data Processing Agreement*.

13.2. Both Parties shall be entitled to require this *Data Processing Agreement* renegotiated if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.

13.3. The Parties agreement on remuneration, terms etc. in connection with amendments to this *Data Processing Agreement*, if applicable, shall be specified in the Parties *Main Agreement*.

13.4. This *Data Processing Agreement* may be terminated according to the terms and conditions of termination, incl. notice of termination, specified in the *Main Agreement*.

13.5. This *Data Processing Agreement* shall apply as long as the processing is performed. Irrespective of the termination of the *Main Agreement* and/or this *Data Processing Agreement*, the *Data Processing Agreement* shall remain in force until the termination of the processing and the erasure of the data by the *Data Processor* and any sub-processors.

14 Categories of data subjects

14.1. The *Data Processor* processes contact-information on *Data Controller*'s costumers, business and collaboration partners and affiliates, employees and suppliers.

14.2. The *Data Processor* provides a system for the disposal of the *Data Controller* as a hosted service. It is therefore not possible for the *Data Processor* to know of all categories of data subjects.

15 Types of personal data

15.1. The types of personal data:

(15.1.1) IP-addresses

(15.1.2) Domain-names

(15.1.3) Contact and identification information

(15.1.4) E-mail

(15.1.5) Membership information, along with product subscriptions

(15.1.6) Order history and invoices

(15.1.7) Support tickets along with answers

(15.1.8) Phone support call log

(15.1.9) Analytics and usage data

16 Subprocessor

The *Data Controller* approves the use of the specified subprocessors:

Company	VAT	Location	Purpose
Adeo Datacenter ApS	DK37593184	Herstedvang 8, 2620 Albertslund, Denmark	Datacenter, where servers are located
Hetzner Online GmbH	DE812871812	Am Datacenter-Park, 08223 Falkenstein, Germany	Datacenter, where servers are located
Hetzner Online GmbH	DE812871812	Sigmundstraße 135, 90431 Nürnberg, Germany	Datacenter, where servers are located

17 Additional documents

17.1. The *Data Controller* is accepting terms and conditions stated in Additional documents section.

(17.1.1) Terms and conditions: https://speedio.dk/legal/

18 Signature

18.1. The act of signing by the customer serves as verification, confirming their status as an authorized signatory for the company.

18.2. Information about the customer's company:

Company name:

menthea

Company registration number:

DK-26152984

18.3. Signatures for customer and Speedio

Customer located within EU
(the "Data Controller")

Speedio ApS
(the "Data Processor")