Contract for the processing of data on behalf

between

…….
…….
…….

- Principal -

and

EEG Expert
Marco Versace
Erzbergerstrasse 19
22765 Hamburg

- Agent –

1. General

(1) The agent processes personal data on behalf of the principal as defined by Art. 4 No. 8 und Art. 28 of regulation (EU) 2016/679 – General Data Protection Regulation (DSGVO). This Agreement governs the rights and obligations of the parties in relation to the processing of personal data.

(2) If the term "data processing" or "processing" (of data) is used in this contract, the definition of "processing" as defined by Art. 4 No. 2 GDPR is taken as the basis.

2. Subject of the contract

(1) The object of the processing, nature and purpose of the processing, the nature of personal data and the categories of data subjects are set out in Appendix 1 to this contract.

3. Rights and obligations of the principal

(1) The client is responsible within the meaning of Art. 4 No. 7 GDPR for the processing of data on behalf of the agent. The contractor in in accordance with para. 4 para. 6 entitled to inform the client if a data processing which he considers legally inadmissible is the subject of the order and / or a directive.

(2) The principal is responsible for the preservation of the aggrieved party's rights. The agent will inform the principal immediately if the aggrieved party assert their data subject rights to the contractor.

(3) The principal has the right to issue additional instructions to the agent regarding the type, scope and procedure of the data processing at any time. Instructions may be in textual form (e.g. e-mail).

(4) Regulations on any compensation for additional expenses arising from supplementary instructions from the client to the contractor remain unaffected.

(5) The principal may nominate authorized persons. If authorized persons are to be named, they will be named in **Appendix 1**. In the event that the authorized persons change with the principal, the principal will inform the client in writing.

(6) The principal informs the agent immediately if he detects mistakes or irregularities related to the processing of personal data by the agent.

(7) In the event that an obligation to inform third parties under Art. 33, 34 DSGVO or any other statutory duty of registration for the principal exists, the principal is responsible for their compliance.

4. General obligations of the agent

(1) The agent processes personal data exclusively within the framework of the agreements made and / or in compliance with any additional instructions issued by the principal. Exceptions to this are statutory provisions that may oblige the agent to process the data differently. In such a case, the processor shall inform the contracting entity of these legal requirements prior to processing, unless the law prohibits such communication on grounds of significant public interest.
Purpose, type and scope of the data processing are otherwise exclusively based on this contract and / or the instructions of the principal. A deviating processing of data is prohibited to the agent, unless the principal has agreed to this in writing.

(2) The agent commits to carry out the data processing on behalf only in member states of the European Union (EU) or the European Economic Area (EEA).

(3) The agent ensures in the field of order processing of personal data, the contractual processing of all agreed measures.

(4) The agent is obliged to design his company and his operations in such a way that the data which he processes on behalf of the client are secured to the extent required and protected against unauthorized third-party access. The agent will coordinate changes in the organization of the data processing on behalf, in case those are substantial for the security of the data, in advance with the client.

(5) The agent will inform the principal immediately if, in his opinion, an instruction given by the principal violates legal regulations. The agent is entitled to suspend the execution of the mentioned instruction until the instruction has been confirmed or changed by the principal. If the agent can demonstrate that processing according to the instructions of the principal can lead to liability of the agent in accordance with Art. 82 GDPR, the agent is entitled to suspend the further processing until clarification of the liability between the parties has been achieved.

(6) The processing of data on behalf of the principal outside the premises of the agent or subcontractors is only permitted with the consent of the principal in writing or text form. A processing of data for the client in private apartments is, in individual cases, permitted only with the consent of the principal in writing or text form.

(7) The agent will process the data that he processes on behalf of the principal separately from other data. A physical separation is not mandatory.

(8) The agent may appoint person (s) to the principal who are entitled to receive instructions from the principal. If authorized persons are to be named, they will be named in **Appendix 1**. In the event that the beneficiaries of the authorization change at the agent, the agent will inform the principal in writing.

5. Data protection officer of the agent

(1) The agent confirms that he has appointed a data protection officer according to Art. 37 GDPR. The agent will ensure that the data protection officer has the necessary qualifications and expertise. The agent will notify the client of the name and contact details of his data protection officer separately in text form.

(2) The obligation to designate a data protection officer under paragraph 1 may be waived at the discretion of the principal if the agent can prove that he is under no legal obligation to appoint a data protection officer and the agent can demonstrate that there are operational rules governing the processing of personal data compliant with the statutory provisions, the provisions of this contract as well as any further instructions of the principal.

6. The agent’s obligation to notify

(1) The agent is obliged to notify the principal of any breach of data protection regulations or violation of the contractual agreements and / or the instructions given by the principal in the course of the processing of data by him or other persons involved in the processing without delay.
The same applies to any infringement of the protection of personal data processed by the agent on behalf of the principal.

(2) Furthermore, the agent will inform the principal without delay if a supervisory authority acts pursuant to Art. 58 GDPR against the agent, this may also concern a control of the processing that the agent performs on behalf of the principal.

(3) The agent is aware that the principal may be required to report in accordance with Art. 33, 34 GDPR, which provides for notification to the supervisory authority within 72 hours of an incident becoming known.
The agent will support the principal in the implementation of the reporting obligations. In particular, the agent will notify the principal of any unauthorized access to personal data processed on behalf of the principal without delay, but no later than within 48 hours after becoming aware of the access

The notification of the agent to the principal must in particular include the following information:

(a) a description of the nature of the personal data breach, where possible, stating the categories and the approximate number of data subjects, the categories concerned and the approximate number of personal data records affected;

(b) a description of the actions taken or proposed by the contractor to remedy the breach of the protection of personal data and, where appropriate, measures to mitigate their potential adverse effects.

7. The agent's obligation to co-operate

(1) The agent supports the principal in his duty to respond to applications for the exercise of data subject rights in accordance with Art. 12-23 GDPR. The regulations of section 11 of this contract.

(2) The agent participates in the preparation of the lists of processing activities by the principal.
The agent must inform the principal of the information required in this regard in a suitable manner.

(3) The agent shall assist the principal in observance of the obligations set out in Art. 32-36 GDPR, taking into account the type of processing and the information available to the agent.

8. Supervisory powers

(1) The principal has the right to check compliance with the statutory provisions on data protection and / or compliance with the contractual provisions made between the parties and / or compliance by the agent with the instructions of the principal at any time and to the required extent.

(2) The agent is obliged to provide information to the principal, insofar as this is necessary for carrying out the inspection within the meaning of paragraph 1.

(3) The principal may request access to the data processed by the agent for the principal as well as to the data processing systems and programs used.

(4) The principal may, after prior notification and within a reasonable period of time, carry out the inspection within the meaning of paragraph 1 in the place of business of the agent at the usual business hours. The Principal shall ensure that the controls are carried out only to the extent necessary so as not to disproportionately disturb the operations of the agent through the controls.

(5) In the case of measures taken by the supervisory authority, the agent is obliged to provide the principal with the necessary information within the meaning of Art. 58 DSGVO, in particular to inform the principal in terms of the agent's information and control obligations, and allow the respective supervisory authority to carry out an on-site inspection.
The principal is to be informed by the contractor about planned measures in this regard.

9. Subcontracting

(1) The commissioning of subcontractors by the agent is only permitted with the consent of the principal in written form. The agent will indicate all subcontracting conditions already existing for the contract in Annex 2 to this contract.

(2) The agent must carefully select the subcontractor and check before subcontracting that the subcontractor can comply with the agreements made between the principal and the agent. In particular, the agent must check in advance and regularly during the contract period if the subcontractor has taken the necessary technical and organizational measures to protect personal data in accordance with Art. 32 GDPR. The result of the inspection must be documented by the agent and transmitted to the principal upon request.

(3) The agent is obliged to have the subcontractor confirm that he has appointed a company data protection officer within the meaning of § 4f BDSG or Art. 37 GDPR. In the event that no data protection officer has been appointed to the subcontractor, the agent must inform the principal and provide information indicating that the subcontractor is under no legal obligation to appoint a data protection officer.

(4) The contractor must ensure that the provisions agreed in this contract and, if applicable, additional instructions of the client also apply to the subcontractor.

(5) The agent must conclude an order processing contract with the subcontractor that meets the requirements of Art. 28 GDPR.
In addition, the agent must impose the same obligations on the subcontractor for the protection of personal data as are specified between the principal and the agent. The order processing contract must be sent to the client on request in copy.

(6) In particular, the agent is obliged to ensure by contractual arrangements that the power to control (section 5 of this contract) of the principal and of supervisory authorities also apply to the subcontractor and that corresponding control rights are agreed on by the principal and supervisory authorities. It is also contractually agreed that the subcontractor must tolerate these control measures and any on-site checks.

(7) Subcontracts within the meaning of subsections 1 to 6 shall not include services that the agent claims from third parties as a mere ancillary service in order to carry out the business activity. These include, for example, cleaning services, pure telecommunications services without any specific relation to services provided by the contractor to the client, postal and courier services, transport services, security services. Nevertheless, the agent is obliged to ensure, even with ancillary services provided by third parties, that reasonable precautions and technical and organizational measures have been taken to ensure the protection of personal data. The maintenance and care of the IT system or applications represents a subcontract and contract processing subject to approval within the meaning of Art. 28 GDPR, if the maintenance and inspection relates to such IT systems that are also used in connection with the provision of services for the client and in the maintenance of those personal data, that are processed on behalf of the client, can be accessed.

10. Confidentiality obligation

(1) The agent is obliged to protect the confidentiality of data received from the principal in the processing of data for the principal. The agent agrees to implement the

same confidentiality rules as are the responsibility of the principal. The principal is obliged to inform the agent of any special rules for the protection of secrets.

(2) The agent warrants that he is aware of the applicable data protection regulations and that he is familiar with their application. The Contractor further warrants that it has familiarized its employees with the relevant data protection provisions and has undertaken to maintain confidentiality. The agent further warrants that he has, in particular, obliged the employees working in the execution of the work to confidentiality and has informed them of the instructions of the principal.

(3) The obligation of the employees according to paragraph 2 shall be proven to the client upon request.

11. Protection of the rights of individuals affected

(1) The client is solely responsible for the protection of the rights of individuals affected. The agent is obliged to assist the principal in his duty to process applications of persons concerned in accordance with Art. 12-23 GDPR. In particular, the agent must ensure that the information required in this respect are provided to the principal immediately, such that the principal can comply with his obligations under Art. 12 para. 3 GDPR.

(2) Insofar as the agent's participation in the protection of affected individual's rights - in particular information, correction, blocking or deletion - is required by the principal, the agent will take the necessary measures according to the instructions of the principal. The agent will, as far as possible, assist the principal with appropriate technical and organizational measures in order to fulfill his obligation to respond to applications for the exercise of affected individual's rights.

(3) Rules on any compensation for additional expenses at the agent incurred through cooperation services in connection with the assertion of affected individual's rights against the principal remain unaffected.

12. Confidentiality obligations

(1) Both parties commit to treat all information received in connection with the execution of this contract as confidential for an indefinite period and to use it only for the execution of the contract. No party is entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to third parties.

(2) The above obligation does not apply to information which one of the parties has demonstrably received from third parties, without being required to maintain secrecy, or which are publicly known.

13. Compensation

(1) The compensation of the agent is agreed separately.

14. Technical and organizational measures for data security

(1) The agent commits towards the principal to implement the technical and organizational measures required to comply with the applicable data protection regulations. This includes in particular the requirements of Art. 32 GDPR.

(2) The status of the technical and organizational measures existing at the time the contract is concluded is attached as **Annex 3** to this contract. The parties agree that technical and organizational measures may be necessary to adapt to technical and legal conditions. The agent will agree on significant changes that may affect the integrity, confidentiality or availability of personal data, in advance with the principal. Measures that involve only minor technical or organizational changes and do not adversely affect the integrity, confidentiality and availability of personal data may be implemented by the agent without coordination with the principal. The principal may at any time request an up-to-date version of the technical and organizational measures taken by the agent.

(3) The agent will check the effectiveness of the technical and organizational measures he has taken on a regular basis and on an ad hoc basis. In the event that there is a need for optimization and / or modification, the agent will inform the principal.

15. Duration of the contact

(1) The contract begins with signing and is concluded indefinitely.

(2) The contract can be terminated with a notice period of three months to the end of the quarter.

(3) The principal may terminate the contract at any time without notice if there is a serious breach of the applicable data protection regulations or obligations under this contract by the agent, or the agent cannot or does not want to execute an instruction of the principal or the agent refuses access by the principal or the competent supervisory authority in breach of contract.

16. Termination

(1) Upon termination of the contract, the agent must return or delete all documents, data and processing or utilization results that have come into his possession, which are related to the contractual relationship, at the choice of the principal. The deletion must be documented in a suitable manner. Any statutory storage obligations or other obligations to store the data remain unaffected.

(2) The principal has the right to check the complete and contractual return and deletion of the data at the agent. This may also be done by a visual inspection of the data processing equipment at the premises of the agent. The on-site inspection should be announced by the principal a reasonable amount of time in advance.

17. Right of retention

(1) The parties agree that the objection of the right of retention by the agent within the meaning of § 273 BGB with regard to the processed data and the associated data carriers is excluded.

18. Final provisions

(1) If the property of the principal is endangered by measures of third parties (e.g. by seizure or confiscation), by bankruptcy proceedings or by other events, the agent must inform the principal immediately. The principal will inform the creditors immediately about the fact that the data concerned are data processed on behalf of the principal.

(2) For ancillary restrictions the written form is required.

(3) Should individual parts of this contract be ineffective, this does not affect the validity of the remaining provisions of the contract.

_____, the _____	Hamburg, the 3.5.2018
Place Date	
_____	_____
- Principal -	- Agent -

Anlage 1 - Subject of the contract

1. Purpose and purpose of the processing

The contract of the principal to the agent includes the following work and / or services:

Measurement data (reaction times) are transferred from the principal to the agent. Furthermore, patient data is regularly entered, stored and graphically evaluated for symptom tracking.

- The measured data are read from the QIKtest device (third party manufacturer)
- Decryptian and storage of test data
- Analysis of test data and comparison
- Saving and holding the analysis data

2. Type (s) of personal data

The following types of data are regularly the subject of processing:

Master data of the principal: Name, address, phone number and fax, e-mail address, time zone, IP number, title, company, username, password, customer history, contract and payment details.

Master data of the patient: ID, gender, date of birth, IP number, anonymous abbreviation, e-mail address, username, password, therapist abbreviation and measurement data.

3. Categories of affected person

Context of data subjects:
Principal and his patients.

4. Authorized persons with instruction rights of the principal

To be clarified in writing for each case individually.

5. Authorized persons with right to receive instructions at the agent

Marco Versace

Annex 2 – Subcontractors

For the processing of data on behalf of the principal, the *agent* uses services from third parties that process data on its behalf ("subcontractors").

These are the following companies:

Credit card billing:

Stripe Inc.
185 Berry Street, Suite 550
San Francisco CA 94107
USA
www.stripe.com
German subsidiary via www.stripe.com/de in Berlin.

Credit card billing automation:

uCollect,
Business Express Technologies Inc
55 Albert Street, Suite 105
Markham, ON L3P 2T4
Canada
www.ucollect.biz

Invoicing:

Xero Limited
Bank House
171 Midsummer Boulevard
Milton Keynes, MK9 1EB
United Kingdom
www.xero.com

Accounting:

office position e.K.
Inh.: Anja Hahn
Donnerstraße 10, Haus 3
22763 Hamburg
www.office-position.com

Server hosting:

UK Dedicated Servers Limited
Unit 21 West Park 211 Torrington Avenue
Coventry CV4 9AP
United Kingdom
www.ukservers.com

Data back up:

Host-Europe GmbH
Welserstr. 14
51149 Köln
www.hosteurope.de

Appendix 3 - Technical and organizational measures of the agent

The agent takes the following technical and organizational measures for data security within the meaning of Art. 32 DSGVO.

1. Confidentiality

The data processing is performed in the productive system (Live Server) by an external processor.

The buildings hosting the server are equipped with electronic and key-based security system.

Visitors are registered and accompanied by company staff.

Electronic access control systems and personnel monitor and ensure that only authorized persons can access to the respective data center. The access regime is designed restrictively. Security area with entrance control. Access control system with chip cards.

Admission control

Login with user name and password, login with biometric data, anti - virus software server, firewall, intrusion detection systems, data encryption, encryption smartphones, user rights management, user profiling, centralized password sharing, secure password policy, enclosure lock, alarm, key for doors

Permissions are granted by the administrator in a restrictive manner.

The granting and withdrawal of authorizations are assigned according to the security concept.

Granted permissions are checked quarterly.

The allocation of required authorizations is checked on a regular basis.

Passwords have a minimum password length, minimum complexity, which is ensured by password management within the server.

Passwords have to be changed each 6 month

Mobile IT systems and data carriers are encrypted, and IT systems are used to protect against viruses and malware.

Automated intrusion detection systems for email and firewall are in use.

Restrictive handling of user rights, restrictive disclosure of data and careful review of contractors will ensure that requirements regarding data security and GDPR are met.

Access control

Physical deletion of data carriers, deployment authorization concept, minimum number of administrators, logging of access to applications, specifically when entering and deleting data, administration of user rights by administrators.

Differentiated access permissions are set by the administrator in a restrictive manner.

User roles and associated permissions are continuously, but at least quarterly, checked

The rights and accesses of exiting personnel or personnel changing withing the company are being managed by the administrator accordingly.

The number of administrators is limited to the minimum.

Accesses to the EEG Expert application are logged.

The destruction of used media is carried out electronically by multiple secure deletion.

Paper documents are stored in locked rooms and destroyed if necessary with shredders.

Separation

Databases are separated by functions and processing is done by separate processes.

The access of customers to data of other customers is guaranteed by the application EEG Expert as well as by operating system hardening.

Test and production systems are separated physically, the transfer of data and programs is secured with SFTP.

Pseudonymization & encryption

Patient data is protected by pseudonymisation and by reference through a code number. Personal data can only be reconstructed through a disproportionate effort.

2. Integrity

Entry control

Data entry is logged at the application level by means of an event database. This evidence is stored for 6 years and the administrator of EEG Expert has access to this data.

Control of transfer

Personal data is transferred for both customer and patient data only with secure web connections: HTTPS for web offers, SFTP for data transmission, email with TLS.

Data will be securely deleted after the job is completed. Deletions are documented.

3. Availability and resilience

An uninterruptible power supply UPS is in use in server hosting and the rooms are air conditioned. Fire alarm and smoke detector systems are in place. Disk mirroring is used in the backup concept to replicate and restore all data disks.

Data backup consists of daily backup of the application and its data on a second local hard drive, daily backup on external server. Backups are encrypted.

The contingency plan takes place in case of disruption. Regular backup consistency and recoverability checks ensure rapid data recovery.

4. Procedures for periodic review, grading and evaluation

The management of EEG Expert is committed to the responsibility for data protection and information security. Employees are obliged to confidential data protection by written confirmation and information.

The data protection officer is Mr. Marco Versace of EEG Expert.

Technical measures that implement data protection are alarm system on the server, automatic access systems, security locks, firewall and anti-virus software, access control for server administration, encryption, secure password rules, use of intrusion detection systems, use for the physical deletion of data, Secure multi-tenancy implemented in the application, provision of encrypted connections such as SFTP and SSL, logging of data changes and data deletions.

Requests for data protection are handled with priority in the support process, thereby guaranteeing timely implementation.

The list of processing activities is available.