BRAINLAB

Data Protection Agreement ("Agreement")

between

Brainlab AG
Olof-Palme-Str. 9
81829 Munich
Germany
(Contractor)

and

Your Information:

_____

You

_____

_____

_____

Hospital/practice, Street/No., City, State, ZIP, Country, Fax number

(Client)

1. Scope and Object of Data Processing

The Client and the Contractor hereby conclude about the processing, subject to directions, of personal data by the Contractor on behalf of the Client.

This Agreement specifies the User´s agreement regarding the specifications given the by EU Data Protection Directive 95/46/EG (particularly Article 17) and the corresponding national provisions adopted by the European Member States pursuant to the EU Data Protection Directive 95/46/EG relating to the security of data processing on behalf (e.g. Section 11 of the German Federal Data Protection Act – BDSG).

The Contractor makes Quentry Services available, a web based software for medical professionals and associated team members, which provides tools for secure online patient data transfer, review, enrichment and for collaborative working. The objective of the data processing is the performance of the Quentry Services.

The Agreement applies to all activities arising in connection with this Agreement and in which the Contractor's employees, or third parties commissioned by the Contractor, come into contact with Client personal data.

The contents of this Agreement apply accordingly when inspection or maintenance of automated procedures or on data processing systems is carried out and the possibility of access to personal data during such inspection and maintenance cannot be ruled out.

2. Definition of Key Concepts

(1) "Affiliate" shall mean any person or entity which controls, is controlled by or is under common control with another person or entity, for so long as such control exists. For purposes of this section, "control" means (i) in the case of corporate entities, direct or indirect ownership of fifty percent (50%) or more of the stock or shares entitled to vote for

the election of directors, and (ii) in the case of non-corporate entities, direct or indirect ownership of fifty percent (50%) or more of the equity or income interest therein.

(2) “Collection” of Personal Data shall mean the acquisition of data on the data subject.

(3) “Controller” shall mean any person or body which collects, processes or uses Personal Data on his, her or its own behalf, or which commissions others to do the same (responsible entity).

(4) “Directive” is a targeted instruction issued by the Client in respect of a specific manner in which the Contractor works with Personal Data. Existing Directives (e.g. provided by this Agreement) can be amended, supplemented or replaced by individual Directives issued by the Client.

(5) “Personal Data” shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person (data subject). This covers, including but not limited to, Personal Data of Users (e.g. employed physicians and health care personnel) as well as uploaded personal data of patients (e.g. name, patient ID, diagnostic image information).

(6) “Processing” shall mean storage, alteration, transfer, blocking or erasure of Personal Data.

(7) “Processor” shall mean any person or body other than the data subject which processes Personal Data on behalf of the Controller.

(8) “Services” shall mean the services available at Quentry.com.

(9) “Special Categories Of Personal Data” shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

(10) “Use” shall mean any utilization of Personal Data other than Processing.

(11) “User” is any registered person using Quentry.

3. Obligations of the Client

(1) The Client is deemed to be the ‘Controller’. As such, it shall be solely responsible for complying with the applicable statutory requirements relating to privacy, data protection and confidentiality of communication related to its Use of the Quentry Services.

(2) The Client shall in particular be solely responsible for providing legal admissibility for selecting, Processing and using Personal Data or Special Categories Of Personal Data (e.g. data subject has given consent, patient has released doctor from medical confidentiality).

(3) The Client shall be responsible for fulfilling the duties to inform the responsible supervisory authority and the data subject in case Special Categories Of Personal Data or Personal Data subject to professional secrecy has been unlawfully transferred or otherwise unlawfully disclosed to third parties.

(4) The Client will give the Contractor specific Directives via email or through other electronic or online authorization tool via the Quentry Services.

4. Obligations of the Contractor

(1) The Contractor is deemed to be the ‘Processor’ Processing the Client’s Personal Data exclusively within the scope of the aforementioned activity. The Contractor is not authorised to process the Client’s data in other form than instructed.

(2) For the term of the subscription for the Quentry Services the Contractor will, at its election and as necessary under applicable law implementing Art. 12(b) of the EU Data Protection Directive 95/46/EG, either (a) provide the Client with the ability to correct, delete or block Client data by using and operating the Quentry application, or (b) make such corrections, deletions or blockages on the Client’s behalf.

(3) Within the Contractor’s scope of responsibility, the Contractor shall take the appropriate technical and organizational measures to adequately protect the Client’s Personal Data against misuse and loss in accordance with the requirements of the EU Data Protection Directive 95/46/EG. Such measures are set out in **Appendix 2**. The Contractor regularly monitors compliance with these measures.

(4) Notwithstanding the provisions of 4.(3) above, the Client acknowledges that the Contractor may, as part of ongoing system maintenance and development, change its appropriate technical and organisational protection measures. The Contractor shall not provide security controls that deliver a level of security protection that is lower than that provided as at the Effective Date but, in any event, the level of protection as required under the EU Data Protection Directive 95/46/EG, particularly Article 17.

(5) The Contractor shall ensure that any Contractor personnel entrusted with Processing the Personal Data have undertaken to comply with the principle of data secrecy and do not pass on, or otherwise make use of information pertinent to the Client to third parties.

(6) The Contractor shall without undue delay, inform the Client in case of a serious interruption of operations or violation of Personal Data protection.

(7) Where the Client, based upon applicable data protection law, is obliged to provide information to a data subject about the Collection, Processing or Use of its Personal Data the Contractor shall assist the Client in making this information available, provided that (a) the Client has instructed the Contractor in writing to do so, and (b) the Client reimburses the Contractor for the costs arising from this assistance.

(8) Should a data subject or a data protection authority make any queries or requests concerning the subject matter of the User Agreement – irrespective of the form of the query (orally, by telephone or in writing) – the Contractor shall inform the Client without delay, however within reasonable timeframe. If such queries relate to complaints made by data subjects, the Contractor shall use appropriate measures to ensure that these complaints are treated in compliance with the confidentiality requirements and that these are forwarded to the Client's data protection officer.

5. Confidentiality

The Client and the Contractor shall treat all knowledge of operational and business secrets acquired within the scope of this Agreement with confidentiality. This also applies, should individual contracts or business relations between the parties be terminated.

6. Data Protection Officer

The Contractor appointed a specialised and qualified data protection officer and shall inform the Client of the officer's name and contact details on request.

7. Subcontractors

(1) The Client explicitly consents to the Contractor deploying subcontractors providing Services on behalf of the Contractor, e.g. such as customer support if subcontracting complies with the following:

Any such subcontractors will be permitted to obtain Client data only to deliver the Services the Contractor has retained them to provide, and they are prohibited from using Client data for any other purpose. Any subcontractors to whom the Contractor transfers Client data, even those used for storage purposes, will have entered into written agreements with the Contractor requiring that the subcontractor abide by terms no less protective than this Agreement. Except as set forth above, or as the Client may otherwise authorize, the Contractor will not transfer to any third party Personal Data the Client provides to the Contractors through the Use of the Quentry Services.

(2) With regards to the aforementioned, the Client hereby explicitly consents to the subcontracting of Services to Affiliates of Contractor and to third parties to fulfil its contractual obligations resulting from this Agreement. The relevant subcontractors are listed on Quentry under the help page in a separate document. Contractor will update the applicable website in the event of any changes with respect to subcontractors.

8. Client Monitoring

(1) The Client or an appropriately authorised party has the right to monitor the Contractor's compliance with the technical and organizational measures.

(2) To enable such monitoring the Contractor will, upon request, provide the Client with voluntary disclosures from the Contractor or certification statements by an independent third party or expert's opinion respectively, detailing the Contractor's compliance with industry information security standards.

(3) Upon the Client's reasonable belief that the Contractor is not in compliance with its security policies and procedures under this Agreement or if such a monitoring is required by the Client's data protections regulators, an appropriately independent auditor selected by the Client at the Client's expense may conduct an on-site monitoring of the Contractor's architecture, systems and procedures used in connection with the Quentry Service during regular business hours, without disrupting the Contractor's business operations. Such monitoring may be conducted up to one time per year, with at least three week's advance notice. After conducting such monitoring, the Client must notify the Contractor of the manner in which the Contractor does not comply with any of the data protection and/or data security obligations herein, if applicable. Upon such notice, the Contractor shall use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

(4) If any audit under this section requires the equivalent of more than one business day of time, expended by the Contractor, the Client agrees to reimburse the Contractor for any additional time expended at the Contractor's then current professional services rates.

9. Client Data Deletion or Return

The Client is responsible for removing its Personal Data from the Services. The Client does not hand out any data storage media to the Contractor.

10. Term and Termination Rights

The term of this Agreement is perpetual and complies with the User Agreement.

11. Waiver

The Client explicitly waives a necessary receipt of Contractor`s notice of acceptance of Clients offer to enter into this Agreement (Sec. 151 phrase 1 German Civil Code).

12. Miscellaneous

(1) Amendments to this Agreement must be agreed in writing. The written form requirement also applies to changes of the written form requirement. The written form requirement does not apply, if it is overruled on the basis of a specific and individual agreement between the parties.

(3) This Agreement shall be governed by German law excluding conflict of laws provisions. Exclusive place of jurisdiction shall be Munich, Germany.

(5) If any provision of this Agreement, or the application thereof to any person or circumstance, is held invalid, such invalidity will not affect any other provision which can be given effect without the invalid provision or application and to this end the provisions hereof will be savable. The invalid clause shall be replaced by such valid clause, which comes closest to the commercial intention of the parties.

13. Appendices

The following appendices form a component part of this Agreement.

- Appendix 1: A list of Personal Data elements and the purpose of their Processing by Contractor on behalf of Client.
- Appendix 2: Overview of the technical and organizational measures taken by Contractor.

BRAINLAB

Location, Date	Location, Date
	Rainer Birkenbach Digitally signed by Rainer Birkenbach DN: o=Brainlab AG, email=rainer.birkenbach@brainlab.com, cn=Rainer Birkenbach Date: 2017.08.21 14:13:05 +02'00'
Signature, Stamp Client	Signature, Stamp Contractor

BRAINLAB

Appendix 1:

A description of the Contractor's activities, including a description of the type of the data and the circle of data subjects.

1. Purpose of Processing Personal Data

Contractor makes Quentry available, a web based software for medical professionals and associated team members, which provides tools for secure online patient data transfer, review and enrichment and for collaborative working.

2. Type of data

- Personal Data of Users
  - full name
  - academic title
  - address (street, city, postal code, state)
  - department
  - position
  - email
  - any user name
  - any password
  - task in CareTeam (where applicable)
  - IP-address (anonymized)

- Personal Data of patients
  - full name
  - date of birth
  - gender
  - patient ID
  - diagnostic image information
  - accession number
  - study description
  - study date
  - patient comments
  - any information concerning the patient in attached files

3. Circle of data subjects:

- Users
- patients

BRAINLAB

Appendix 2:

Overview of the technical and organisational measures taken by Contractor

Within its area of responsibility the Contractor takes the following technical and organizational measures during Processing Personal Data:

• Access control to premises and facilities

The Contractor and involved cloud platform providers take in particular the following measures to prevent unauthorized persons from gaining access to data processing systems for Processing or using Personal Data:

The physical access to the Contractor's premises including the data centers is ruled through formal access procedures. The access to Contractor's premises or data centers and restricted zones respectively requires proper identification and is limited to authorized personnel based on job function. Visitors have to register in a visitor's log sheet and have to wear a visitor's badge with temporary and restricted access rights. Visitors are escorted by security personnel. Additionally, security measures are implemented such as video-surveillance and security guard.

• Access control to systems

The Contractor takes in particular the following measures to prevent data processing systems from being used without authorization:

For User identification and authentication: User ID, password procedures incl. password complexity requirements, reset of generated initial password on first use, periodic change of password, password history controls and automatic blocking (e.g. password request or timeout). A Quentry User session expires automatically after a period of inactivity. The Quentry system is hosted on Amazon Web Services (AWS). The Contractor uses the AWS Identity and Access Management to ensure that only specifically appointed and authorized employees of the Contractor have access to the Quentry system for support and maintenance. All Users with elevated access rights will be required to use AWS Multi-Factor Authentication. On network level the AWS Security Groups (firewall) are configured to restrict administrative access to the Quentry system only to inbound connections from the secured network of the Contractor.

salesforce.com is utilized for User authentication (storage of User name and password). The network connection from the Quentry system to the salesforce.com system is encrypted via SSL. The passwords are stored encrypted.

• Access control to data

The Contractor takes in particular the following measures to ensure that persons authorised to use data processing systems have access only to those data they are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during Processing, Use and after recording:

Administrative access to the Quentry system and stored Personal Data is granted for a very limited number of employees of the Contractor. The assigned authorizations are based upon job responsibilities and provisioned to least privilege. Such access is granted to restart the Services and any other activity to maintain a secure and operational Quentry system. Remote access is configured in the firewall (AWS security group) to allow access only from the Contractor's network.

Data uploaded by Users is split up and stored fragmented on different server instances. All processed files are stored encrypted either with the Advanced Encryption Standard (AES 256) or using BitLocker Drive Encryption. The correspondi**n**g encryption key is stored encrypted on another virtual machine. As only the Contractor processes the encryption keys, cloud platform providers do not have access to view decrypted data. A multi-tenant system is employed which ensures that a User cannot access Personal Data of another User unless the other User gives the approval through setting granular sharing permissions via the Quentry system.

• Data transfer control

The Contractor takes in particular the following measures to ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media,

and that it is possible to ascertain and check to which parties Personal Data is transferred to.

The communication between the User client and the Quentry system is secured through SSL certificate (issued by GlobalSign, minimum 128-bit to 256-bit encryption, depending on client capabilities) and a session ID generated by the Quentry system. The session ID is created during the login process and is only valid for the period the User is active.

• Entry control

The Contractor takes in particular the following measures to ensure that it is possible after the fact to check and ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so, by whom:

An event log is implemented tracking the Use of the Quentry system by the User. The log documents access and Use of Quentry containing Client data, including the access ID, time, authorisation granted or denied, and relevant activity.

• Control of instructions

The Contractor takes in particular the following measures to ensure that Personal Data processed on behalf of the Client is processed in compliance with Client's instructions:

As set forth in the Data Protection Agreement, the Contractor shall process Personal Data of the Client in accordance with the instructions of the Client. Further, the Contractor has concluded data protection agreements with relevant subcontractors complying with the specifications given by EU Data Protection Directive 95/46/EG and the German Federal Data Protection Act. Prior to the commencement of Processing, and in regular intervals thereafter the Contractor monitors the technical and organizational measures taken by the subcontractors.

• Availability control

The Contractor takes in particular the following measures to ensure that Personal Data are protected against accidental destruction or loss:

The Contractor uses a combination of redundant systems, firewall, anti-virus solution, intrusion detection system and data security as well as backup solution, to protect - and if necessary restore - the Client's Personal Data. A backup and disaster recovery concept describing the relevant procedures as well as responsibilities of personnel is in place. Disaster recovery is tested regularly.

• Separation control

The Contractor takes in particular the following measures to ensure that data collected for different purposes can be processed separately:

Client's Personal Data is processed on server systems, which are logically separated within the network. A strong logical separation of Client data is achieved via client-specific User IDs that permits only authorized Users to view related Client data.

Client may implement a granular sharing model and User permission profiles to limit data access to different Users.