EuroPriSe European Privacy Seal

Short Public Report

1. Name and version of the IT-based service:

- Quentry, Version 2.0
- Quentry Desktop, Version 3.0
- Quentry Gateway, Version 3.0

2. Provider of the IT-based service:

Company Name:	Brainlab AG
Contact Person:	Michaela Oberrecht-Heusler, General Counsel
Address:	Kapellenstr. 12 85622 Feldkirchen Germany

3. Time frame of evaluation:

05 December 2013 to 19 January 2016

4. EuroPriSe Experts who evaluated the IT-based service:

Name of the Legal Expert:	Johanna Laas
Address of the Legal Expert:	intersoft consulting services AG Beim Strohhause 17 20097 Hamburg Germany
Name of the Technical Expert:	Dr. Michael Foth
Address of the Technical Expert:	IBS Schreiber GmbH Zirkusweg 1 20359 Hamburg Germany

5. Certification Body:

Name:	EuroPriSe Certification Authority
Address:	Joseph-Schumpeter-Allee 25
	53227 Bonn
	Germany
eMail:	contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

- IT-based service Quentry® – (Version 2.0)
- IT-Product Quentry Desktop – (Version 3.0) using the IT-based service Quentry® – (Version 2.0)
- Quentry Gateway - (Version 3.0) using the IT-based service Quentry® – (Version 2.0) (facilitating pre-configured automatic upload from user-side)
- System-Architecture and Cloud-Processing relying on Quentry's multilayered encryption solution
- Interface and User-Authorization by means of Salesforce authentication services, but not Salesforce cloud services as such
- Key handling and encryption management
- De-Identification-Process
- Administration und Support by Brainlab AG and Brainlab Ltd.
- IT-Components hosted by Amazon, but not Amazon cloud services as such

NOT part of ToE:

- Quentry App for iOS
- Application TraumaCad Web
- Hardware used by customers
- Third party networks

7. General description of the IT-based service:

Quentry is a Brainlab cloud-based service for image sharing and collaboration. This service gives hospitals, clinics, imaging centers and physicians the freedom to access, control and share diagnostic imaging from anywhere within a secure clinical network. Built on a secure infrastructure, Quentry connects experts from radiology to surgery to radiotherapy and supports clinicians throughout the referral, diagnosis, planning and treatment workflow.
Quentry provides timely access to patient information available from any outside facility, such as imaging centers or any referring institutions.

For patient data processed by Quentry, the users each qualify as individual controller in accordance with EU Directive 95/46/EC, meaning that the user is responsible for processing their patient data and determines the purpose and means of the processing.
Brainlab as a separate legal entity acts as a service provider and therefore as the processor of the patient data.

For user data such as user name and address, Brainlab is responsible for the lawful processing as controller in accordance with EU Directive 95/46/EC.

8. Transnational issues:

The service is offered in countries in the EU/EEA as well as in countries outside the EU/EEA.
Data transfers outside the EU/EEA are secured through additional measures such as EU model clauses or consent of data subjects where applicable.

9. Tools used by the provider of the IT-based service:

Quentry service

- Microsoft .NET Framework v4.5 SP1 or higher
- Microsoft IIS
- Microsoft SQL-Server 2012

- Javascript libraries (running on the browser)
- Owin

Quentry Desktop

- Microsoft .NET Framework v4.5 SP1 or higher

Quentry Gateway

- Microsoft .NET Framework v4.5 SP1 or higher
- Internet Information Services (IIS)
- Windows Communication Foundation HTTP Activation
- Windows Communication Foundation Non-HTTP Activation
- ASP.NET 2.0 enabled (following installation of .NET Framework and IIS)

10. Version of EuroPriSe Criteria catalogue used for the evaluation:

Version November 2011

11. Evaluation results:

a. Overview of fundamental issues

Quentry complies with all legal requirements of EU Directive 95/46/EC and EU Directive 2002/58/EC, the requirements established by the Art. 29 Data Protection Working Party as well as with national laws, where applicable and also sets high standards in regard to the technical security of the processed data.

Processing operations of Quentry regarding user and patient data are the registration process (user data), login (user data), data upload via web uploader, gateway or desktop, view and download (patient data) and processing files on the Quentry server (patient data).

Users can chose to de-identify the (patient) data during the upload process to the Quentry platform. In all cases patient consent is required, which the user must confirm before uploading any data.

User data is solely collected and processed for registration and authentication purposes.

To avoid communication with other users, users can set their profile as "invisible" which means they will not appear in the search results and other Quentry users cannot add them as a contact.

Therefore, the processing of (user and patient) data remains at all times strictly limited to the legitimate purpose of the relevant data processing operation. The service complies with the concept of Data Avoidance and Minimisation.

The Quentry website is well-structured, so that it is easy for users to find service, help and data protection information. The Privacy Policy provides information about data processing as well as the responsibility of the user regarding patient data, the requirement of patient consent and release from medical confidentiality.

The User Guides and product descriptions are also easily understandable without special knowledge. The Privacy Hints document provides details about data protection features of Quentry and how to use the service in a privacy compliant manner.

b. Legitimacy of data processing

Brainlab designed the Quentry platform in a privacy enhancing way.

Regarding user data, Brainlab is the controller. Legally, the controller is "processing on the basis of a contract", Article 7 (b) Directive 95/46/EC because the user concludes a contract with Brainlab by using the platform. Brainlab only collects and processes user data, which is necessary to perform the service or to comply with legal obligations from the medical sector (e.g. Directive 93/42/EC concerning medical devices). Data is deleted as soon as the purpose of collection is fulfilled. An erasure workflow exists.

Regarding patient data, the user is the controller and must obtain the necessary consent from the patient. Brainlab acts as a service provider in this regard.
Therefore, users must conclude the Data Protection Agreement relating to commissioned data processing (Art. 17(2)-(4) Directive 95/46/EC) with Brainlab in order to use the Quentry platform. This is ensured through a workflow with a qualified electronic signature and a reoccurring pop-up which reminds the user to confirm the contract.
Data protection agreements in accordance with Art. 17(2)-(4) EU Directive 95/46/EC, including appropriate technical and organisational measures have been concluded with external service providers.

c. Technical-Organizational Measures

Quentry employs advanced encryption and access control technologies to ensure that all sensitive medical information is protected. Data uploaded and stored on Quentry can only be accessed and viewed by the individuals that are authorized to view patient related data through login accounts. Quentry users are in full control over their login credentials. Users can grant access to their patient data to their confirmed contacts in Quentry.

Quentry is designed to protect its patient data from security breaches and malicious attacks. The sophisticated security measures and architecture implemented in Quentry are designed in accordance with European Union Data Protection Directives and meet both HIPAA and HITECH requirements for PHI (Protected Health Information).
All patient data are protected by a multi-layered encryption-system, which secures against unjustified inspection. Service providers and administrators are not able to individually decrypt data.
All communication between the ground components and the providers are secured over TLS communication. For the TLS communication a certificate from GlobalSign created for quentry.com is used and also used for TLS-Webserver-Authentification and TLS-Web-Client-Authentification.

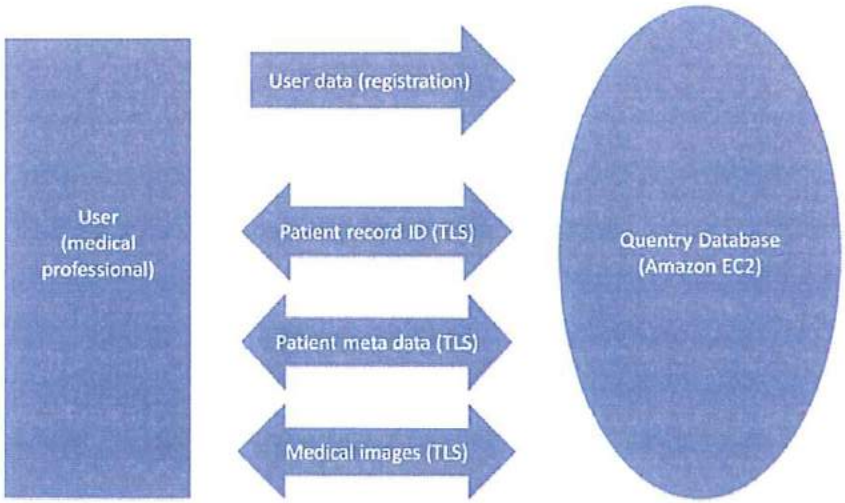
Detailed risk analysis with defined measures is provided for Quentry Desktop, Quentry Gateway and Quentry Cloud service. They are updated regularly or on demand in the case new threats will arise.

d. Data Subjects' Rights

Quentry complies with the concepts of Rights of Erasure, Blocking and Right of Objection to processing of data and ensures that data will be erased when no longer required in accordance with EU Directive 95/46/EC. Personal user data can be edited at all times by the user and is erased upon request. Workflows for data deletion and certain (internal) workflows for data breaches and user inquiries exist.

12. Data flow:

The implemented architecture of Quentry contains a multi-layered encryption system which - in regard to the risks - approximates to the greatest extent possible to the security of an end-to-end encryption. The encryption system is described below.



- All communication between the user (client) and the Quentry-server is secured over TLS with a certificate from GlobalSign.
- User data and patient data are encrypted during transmission to the Quentry-server by TLS communication.
- User login process (External Authentication Service) is encrypted and secured by TLS-Webserver-Authentification and TLS-Web-Client-Authentification.
- Patient data is encrypted in the CPU/RAM of the Quentry-server through a multi-layered encryption process.
- Only after the patient data is encrypted, the data is stored in a secured environment.

13. Privacy-enhancing functionalities:

The Quentry service does provide significant privacy enhancing functionalities. Multi-layered encryption technologies and secure storage of patient data in the cloud demonstrate a high level of protection against unauthorized access.

Patient data are encrypted in a way that under standard conditions no Brainlab employee has access to it. Only in case of major database maintenance or system restoration activity, a decryption of the database might be necessary. A secured process ensures the coordinated decryption and re-encryption of the database. The involvement of several people is required to initiate this process. This includes the database administrator and general management. The access is reviewed in regular data protection audits by the data protection officer and risk management.

It is the user's responsibility as stated in the Quentry terms and conditions, in the Privacy Policy and Privacy Hints document to ensure patient consent before uploading data to the Quentry platform.

The chosen form of architecture of encryption in conjunction with organizational instructions and contractual provisions examined by the legal and technical expert fulfills the technical and legal requirements.

14. Issues demanding special user attention:

The user - as being "controller" - is responsible for the collection of consent and release from medical confidentiality from the patient. However, Brainlab advises and requires the user within the upload process to confirm that user obtained consent and release from medical confidentiality from the patient. This holds true even if only de-identified patient data are processed, because images themselves qualify as personal data. Users must confirm that they obtain their patients' consent beforehand when uploading patient data. The requirement of patient consent is mentioned in several documents on the website such as Privacy Hints and Privacy Policy in order to assist the user to act in compliance with applicable data protection regulation. When obtaining

patients' consent, users must inform data subjects about the following in particular:

- Patient data are processed in the cloud.
- Brainlab processes patient data as a processor on behalf of the user. A controller – processor agreement is in place.
- Brainlab relies on Amazon Web Services as cloud provider (sub-processor). Encrypted patient data are stored in a data center in Ireland only. Sub-processors responsible for maintenance issues may be located in third countries outside of the European Economic Area (EEA). Standard contractual clauses between Brainlab and Amazon Web Services are in place.
- No end-to-end encryption is in place, because this is technically not feasible in this constellation (reason: data are processed in the cloud). However, a sophisticated encryption solution of (nearly) similar quality has been developed and implemented.
- Brainlab is capable of decrypting encrypted patient data, but safeguards are in place that this is only done in exceptional cases such as major database maintenance or system restoration. A secured process ensures the coordinated decryption and re-encryption of the database. Individual employees of Brainlab are not able to decrypt patient data on their own.
- If applicable: That the user shares patient data with hospitals / doctors in countries outside of the EEA which do not provide an adequate level of data protection.

Users must verify that another user with whom they want to connect and share images is in fact the person they claim to be. They must confirm that they verified the identity of the other user when establishing the connection with him. Users must conclude a controller – processor agreement (data protection agreement available on the Quentry platform) with Brainlab prior to uploading any patient data to the cloud. Users must adhere to all relevant national provisions on patient data.

Brainlab uses Salesforce as a service provider for the authentication of users (customers). For the time being, Brainlab relies on standard contractual clauses (SCC) for this transfer of minimum personal data to the U.S.

Brainlab will adhere to future guidance of the Article 29 Working Party regarding the impact of the Safe Harbor judgement on the eligibility of SCC to legitimize international data transfers. For the sake of clarification: Salesforce does not have access to patient data at any time.

15. Compensation of weaknesses:

Not applicable.

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	Adequate	The service only processes personal user data which is needed for the performance of the service and allows the user to de-identify patient data.
Transparency	Excellent	Informative and understandable user guides and service descriptions as well as a detailed privacy policy exist and are easily accessible on the website.
Technical-Organisational Measures	Excellent (regarding encryption solution)	- Patient data are encrypted. - Providers do not have access to the encrypted patient data and have no possibility to get access to the multi-layered encryption-keys.

	Adequate (regarding other measures)	- Risk-analyses for the products exist. - The client-server communication and the internal server-to-server communication are well encrypted. - Organizational measures for incidents, instructions and confidentiality of personnel, vulnerabilities are well documented, controlled and secured by audits. - The de-identification is technically possible and is in addition to confirm by the user for every upload. The implemented architecture of Quentry contains a multi-layered encryption system which - in regard to the risks approximates to the greatest extent possible to the security of an end-to-end encryption.
Data Subjects' Rights	Adequate	- Users can access and edit their data at all times. - User data is deleted when requested by the user. - A "user request" workflow regarding data protection inquiries exists. - Workflows exist which notify the user in case of personal data breaches. - The service allows the user to delete patient data at any time.

Experts' Statement

We affirm that the above-named IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Hamburg, 31/03/2016	Johanna Laas	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Hamburg, 31/03/2016	Michael Foth	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Certification Result

The above-named IT-based service passed the EuroPriSe evaluation.

It is certified, that the above-named IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Bonn, 06/04/2016	EuroPriSe CA	
Place, Date	Name of Certification Authority	Signature