Short Public Report

Recertification No. 2

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

Haemoassist® 2, Version 2.7

Functions as provided upon finalisation of the evaluation (February 2019)

2. Manufacturer / Provider of the IT-based service:

Company Name:

StatConsult Gesellschaft für klinische und Versorgungsforschung mbH

Address:

Halberstädter Str. 40a

39112 Magdeburg

Contact Person:

Jan Reichmann

3. **Time frame of evaluation:**

Evaluation started: July 2018

Evaluation ended: February 2019

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

Name of the Legal Expert:

Jörg Joachim Schließke

Address of the Legal Expert:

TÜV Informationstechnik GmbH

Langemarckstraße 20

45141 Essen

Name of the Technical Expert:

Tobias Mielke

Address of the Technical Expert:

TÜV Informationstechnik GmbH

Langemarckstraße 20

45141 Essen

5. Certification Authority:

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

6. Specification of Target of Evaluation (ToE):

Haemoassist® 2 is a smart-phone based therapy management application for Hemophiliacs and their physicians. It consists of an electronic patient diary (application) in conjuncture with a web-based monitoring-interface for the attending physicians.

The target of evaluation consists of the following components:

- Provisioning of the electronic patient diary as well as the portal for physicians and the web interface for patients
- The user registration process
- All IT-systems necessary for providing the electronic patient diary and the browser based application portal
- Relevant contractual regulations

Excluded from the target of evaluation are the following:

- IT systems (clients) used by physicians, the smartphones and PC that are used by patients to gain access to the Haemoassist® 2 service.
- Networks or active network components, further IT-systems that are used to transfer or handle data.

7. General description of the IT-based service:

Haemoassist® 2 is a smart-phone and web based therapy management application for Hemophiliacs and their physicians. It consists of an electronic patient diary (application) in conjuncture with a web based monitoring-interface for the attending physicians. The Haemoassist® 2 service compiles and stores data from patients and physicians that concerns the type of therapy and the development of the medical condition. This data is stored on the patients' smartphones and on the central databases and is depersonalized to ensure confidentiality. There are no fields containing directly identyfying personal information. The identification of patients is implemented by a process of pseudonymization.

8. Transnational issues:

The Haemoassist® 2 service is limited to EU-member states and the data are stored in IT-servers that are located only in Germany. The storage of personal

data takes place only in Germany but the Haemoassist® 2 service can also be used by patients who live in Austria, Denmark and other countries of the European Union.

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

The purpose of the IT-based service Haemoassist® 2 is to provide an online documentation for haemophilia patients and their physicians. The provider uses tools to supply the IT based services. Those tools are necessary for providing the electronic patient diary and the web (browser) based application portal (servers, network components, memory) for patients and physicians as well as the necessary software (operating systems, databases, application software, web-interfaces). Operating systems and databases itself will not be certified - only the information processing necessary to provide the IT-based service using these components will be certified.

10. Edition of EuroPriSe Criteria used for the evaluation:

The experts used EuroPriSe Criteria Catalogue, version 01/2017.

11. Modifications / Amendments of the IT product or IT-based service since the last re-certification

The following new technical functionality updates have been implemented for the service

<u>Notes from the Patient</u>:

The patient or user has the possibility to gather some notes for factor supplements and haemorrhages into the application. They can comment haemorrhages or unscheduled factor supplements to discuss it with their physician. The notes will be stored encrypted and only the physician have access to these notes. The notes are visualized in the individual patient view and calendar view. The patient will be informed by the application before his first usage. This information-button is always invocable.

Delivery workflow for medication:

The physician has the possibility to document the tracking number of the parcel consigner into the medication dispenser in the application.

The patient will be informed about new medication shipment. A hyperlink to the parcel consigner is available to view the shipping announcement. He has got also the view to see the medication shipment of the last 30 days.

12. Changes in the legal and/or technical situation

There are significant changes in the legal national and international framework. Since 25. May 2018 the Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) is applicable and replaces the Data Protection Directive 95/46/EC. The certification body has published a criteria catalogue in 01/2017 that was used for this recertification. This criteria catalogue already reflects the legal requirements of the GDPR, but it has not been approved in accordance with Art. 42 (5) GDPR.

13. Re-Evaluation methods:

The following evaluation methods were used:

- Interviews
- Document reviews
- Workshop and on-site audit in Magdeburg
- Online audit of the website
- Function and security analysis tests of the iOS and Android App

14. **Re-Evaluation results**:

Every patient must sign a declaration of consent before he can use the Haemoassist® 2 service. His physician preserves one copy of the declaration remains with the patient, a second copy. The declaration of consent is part of the patient´s “Welcome Package” that contains a detailed and understandable description of the Haemoassist® 2 service. No form of duress, offers of

advantages or disadvantages or threats are used in the declaration of consent. The consent is given freely.

Booklets as part of the “Welcome Package” inform the patient of the purpose of processing (efficient therapy management) and give some further information regarding data collected by himself via app or web interface and the possibility of his physician to access the patient´s diary/data.

According to Art. 13 and 14 of the GDPR the data subjects have to be informed about data processing activities and further details for a transparency process. Patients are given detailed information about the Haemoassist® 2 service in their “Welcome Package” and additional documents describing privacy issues of the web access by patients, e.g.:

• Overview of the service and its interfaces, pseudonymization, technical security measures

• Functionality of the patient´s app and web interface; detailed description of every field (instruction manual)

• A flyer describing how to install the app. The patient is explicitly advised that the first step is to sign the declaration of consent and that without this consent the Haemoassist® 2 service cannot be used.

• Declaration of consent to be signed by the patient. The patient is advised that he can object to processing by contacting his physician. Subsequently the physician would contact StatConsult in order to de-activate the patient´s account and the physician´s right to access the patient´s diary by app or web interface.

The security of remote access to the product is comparable to the internal access because VPN tunnelling is used if remote administration access is necessary. The identity of recipients is verified and the transmission of authorization data is secured. Before any data is transmitted over the network

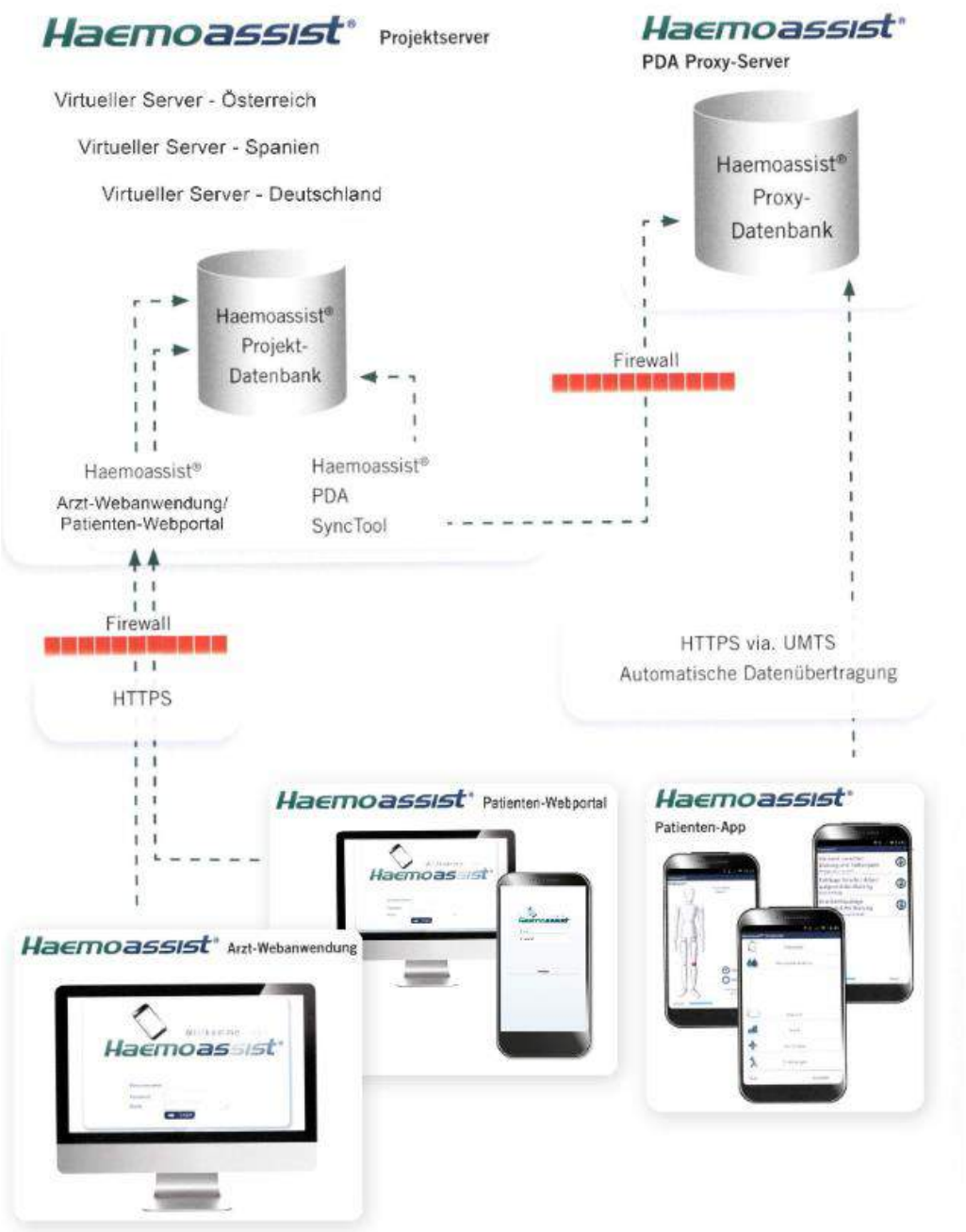
the data is encrypted. Internal networks are secured by a firewall and parts of the network that are accessible from the outside are specifically shielded.

Unauthorized disruption of power or network lines is prevented by different security instances in the data center. Unauthorized personnel cannot access the data center, which is lying under the surface. Maintenance Service is done on a regular basis. All data is backed up on a regular basis. Backups are encrypted and backup restore procedures are tested on a regular basis.

The App "Haemoassist" uses an encrypted HTTPS connection for communication.

The application saves data in the app directory intermediately. The access rights to this directory are set restrictively by the operating system so that only the app itself can access it.

15. Data flow:



16. Privacy-enhancing functionalities:

The Haemoassist® 2 IT-based service uses only pseudonymized data: the patient´s name is not stored in the database of the service but is known only to the patient and his physician. Data is pseudonymized by using a specific patient ID for each patient. The correlation of the patient´s name to the patient´s

specific ID is only known to the patient and his physician. Before the transportation of the data through networks, it is encrypted. The transportation is done via HTTPS.

17. Issues demanding special user attention:

Patients and physicians should pay special attention to privacy related issues of their IT systems (smart-phones, clients, PC, etc.), as these items are not included into the ToE.

18. Compensation of weaknesses:

Not relevant

19. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	adequate	service makes use of pseudonymisation
Transparency	excellent	patients are provided easy to access and detailed information about the Haemoassist® 2 service offline and online
Technical-Organisational Measures	adequate	service uses only pseudonymized data; data is encrypted
Data Subjects' Rights	adequate	patients are provided detailed information on the data subject´s rights in the "welcome package", privacy relevant documents can be downloaded via web interface

Experts' Statement

We affirm that the above-named IT product / 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.

Essen, 07 March 2019	Jörg Joachim Schließke	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Essen, 07 March 2019	Tobias Mielke	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Recertification Result

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

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

Place, Date	Name of Certification Authority	Signature