Short Public Report

Recertification No. 1

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

   Haemoassist® 2, Version 2.4

   Function as provided upon finalisation of the evaluation (August 2016)

2. Provider of the IT-based service:

   Company Name:

   StatConsult Gesellschaft für klinische und Versorgungsforschung mbH

   Address:

   Halberstädter Straße 40a

   39112 Magdeburg

   Contact Person:

   Jan Reichmann

3. Time frame of evaluation:

Evaluation started: August 2015

Evaluation ended: August 2016

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

Name of the Legal Expert:

Hannelore Jorgowitz

Address of the Legal Expert:

PERSICON consultancy GmbH

Friedrichstraße 100

10117 Berlin

Name of the Technical Expert:

Knut Haufe

Address of the Technical Expert:

PERSICON consultancy GmbH

Friedrichstraße 100

10117 Berlin

5. Certification Authority:

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):

Haemoassist® 2 is a smartphone and web based therapy management application for

haemophilia patients and their physicians. It consists of an electronic patient diary (application) in interaction with a web based patient access and 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:

- Neither IT systems (clients) used by doctors nor the smartphones and PC that are used by patients to gain access to the Haemoassist® 2 service are included in the evaluation.
- Neither networks or active network components nor further IT-systems used to transfer or handle data are included in the evaluation.

7. General description of the IT-based service:

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 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 its necessary IT-servers are located in Germany only. 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 manufacturer of the IT product / 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. Tools used by the provider to provide the IT-based service consist of IT-systems necessary for providing the

electronic patient diary and the browser based application portal (servers, network components, memory) for patients and physicians as well as the necessary software (operating systems, data bases, 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 this components will be certified.

10. Edition of EuroPriSe Criteria used for the evaluation:

November 2011

11. Modifications / Amendments of the IT-based service since the last (re)certification

A new technical functionality has been implemented for patients. They can access the IT based-service not only via smartphone app but also via web interface. The data are completely transmitted via HTTPS. The web access for patients is secured by login / password and TANs. TAN lists are individually numbered and have an expiration date. Only one TAN list per patient is valid.

12. Changes in the legal and/or technical situation

There are no changes in the legal national or European data protection framework. A new technical functionality has been implemented for patients. They can access the IT based-service not only via smartphone app but also via web interface.

13. Evaluation results:

Every patient must sign a declaration of consent before he can use the Haemoassist® 2 service. One copy of the declaration remains with the patient, a second copy is preserved by his physician. The declaration of consent is part of the patient´s "Welcome package" which 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. 10 and 11 of the Directive 95/46/EC the data subjects have to be informed about data processing activities. 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.:

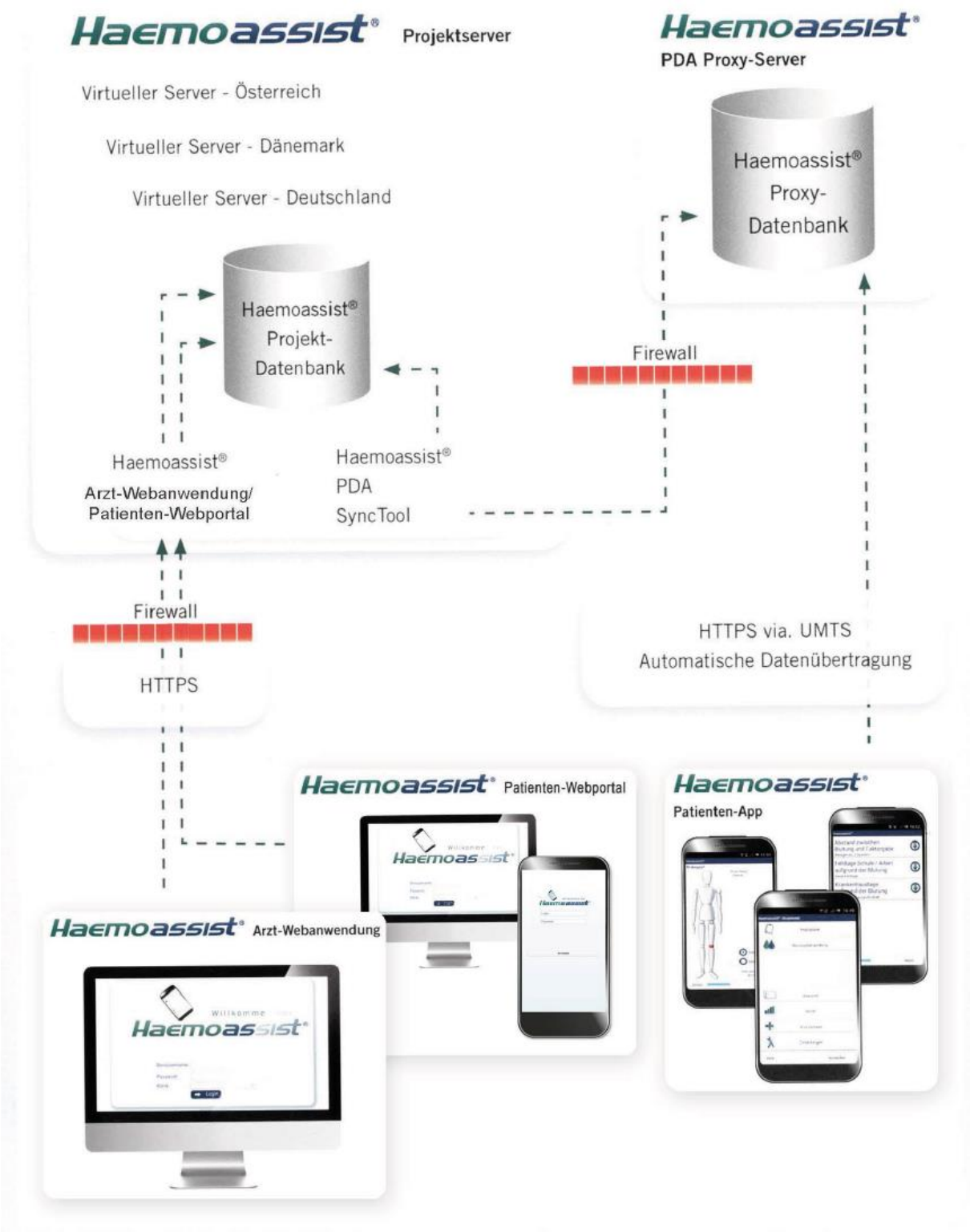
- overview of the service and its interfaces, pseudonymization, technical security measures
- functionality of the patient´s app and web interface; detailed description of every field (instruction manual)
- a flyer describing how to install the app. The patient is explicitly advised that the first step 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
- In the declaration of consent 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.

14. Data flow:


Haemoassist® Projektserver
Virtueller Server - Österreich
Virtueller Server - Dänemark
Virtueller Server - Deutschland
Haemoassist® Projekt-Datenbank
Haemoassist®
Arzt-Webanwendung/
Patienten-Webportal
Haemoassist®
PDA
SyncTool
Haemoassist®
PDA Proxy-Server
Haemoassist® Proxy-Datenbank
Firewall
Firewall
HTTPS
HTTPS via. UMTS
Automatische Datenübertragung
Haemoassist® Patienten-Webportal
Haemoassist® Arzt-Webanwendung
Haemoassist®
Patienten-App

15. 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/her 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.

16. 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.

17. Compensation of weaknesses:

Not relevant

18. 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-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.

Berlin, 23 July 2016	Hannelore Jorgowitz	
Place, Date	Name of Legal Expert	Signature of Legal Expert
Berlin, 23 July2016	Knut Haufe	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Recertification 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.

Place, Date	Name of Certification Authority	Signature