Short Public Report

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

   Haemoassist® 2

   Function as provided upon finalisation of the evaluation (October 2014)

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: 27 June 2013

   Evaluation ended: 01 October 2014

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 smart-phone based therapy management application for haemophilia patients and their physicians. It consists of an electronic patient diary (application) in interaction 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
- 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 smart-phones 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' smart-phones and on the central databases and is depersonalized to ensure confidentiality. There are no fields containing personal information. The identification of the 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 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 are all IT-Systems necessary for providing the electronic patient diary and the browser based application portal (servers, network components, memory) 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. Evaluation results:

Set 1 Overview of fundamental issues

The purpose of the IT-based service Haemoassist® 2 is to provide an online documentation for haemophilia patients and their physicians. No further purposes can be identified with Haemoassist® 2. Only the patient´s physician is able to connect the patient´s ID stored in the provider´s database to the name of the patient. The documentation on it remains exclusively with the physician. The purpose of Haemoassist® 2 is sufficiently specified.

Haemoassist® 2 uses cookies only for session identification of physicians. Further cookies, like buttons, tracing tools, et cetera are not being used.

Every patient automatically receives a “welcome package” from his/her physician describing the Haemoassist® 2 service in detail before he/she can download and use the Haemoassist® 2 app. The patient´s declaration of consent is part of this “welcome package”.

Set 2 Legitimacy of data processing

According to Art. 7(a) of Directive 95/46/EC "personal data may be processed only if the data subject has unambiguously given his consent […]". Consent must be given freely – the patient must have a free choice whether he wants to use the Haemoassist® 2 service of StatConsult Gesellschaft für klinische und Versorgungsforschung mbH. Consent must be specific – the patient must be informed about the purpose of the collection and processing of his data. Blanket consent is not permitted. Consent must be informed – the haemophilia patient must be informed in detail about the processing of data collected and all relevant issues.

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. So 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 and the possibility of his physician to access the patient´s diary/data.

Set 3 Technical and organisational measures

The security of remote access to the product is comparable to the internal access because VPN tunneling 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 backuped on a regular basis. Backups are encrypted and backup restore procedures are tested on a regular basis.

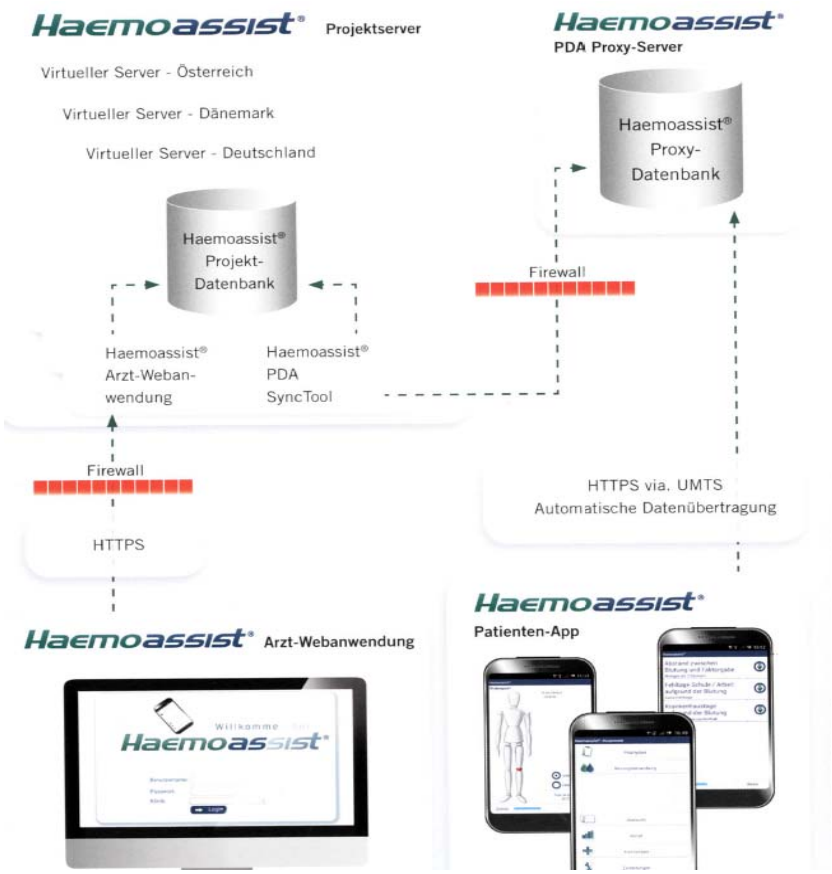
Set 4 Data subjects´ rights

According to Art. 10 and 11 of the Directive 95/46/EC the data subject has to be informed about data processing activities. Patients are given detailed information about the Haemoassist service in their "Welcome package", e.g.:

- overview of the service and its interfaces, pseudonymization, technical security measures
- functionality of the patient´s app; detailed description of every field (instruction manual)
- a flyer describing how to install the app. The patient is explicitely advised that the first step is to sign the declaration of consent and that without this consent the Haemoassist 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.

12. Data flow:



13. Privacy-enhancing functionalities:

The Haemoassist 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.

14. Issues demanding special user attention:

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

15. Compensation of weaknesses:

Not relevant

16. 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 service*
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"*

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, 01 October 2014 Hannelore Jorgowitz

Place, Date	Name of Legal Expert	Signature of Legal Expert

Berlin, 01 October 2014 Knut Haufe

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.

Place, Date	Name of Certification Authority	Signature