SpeechMagic™ Solution Builder Short Public Report

Application No. ULD080009p

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

   "SpeechMagic™ Solution Builder 2.0"

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

   Company Name: Nuance Communications International BVBA

   Address: Guldensporenpark 32, B-9820 Merelbeke, Belgium

   Contact Person: Jan Rusch

3. **Time frame of evaluation:**

   From March 2008 – May 2010

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

   Legal Expert: Stephan Hansen-Oest

   Address: Neustadt 56, 24939 Flensburg, Germany
   sh@hansen-oest.com

   Technical Expert: Andreas Bethke

   Address: Papenbergallee 34, 25548 Kellinghusen, Germany
   bethke@europrise-expert.com

5. **Certification Body:**

   Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein
   Holstenstraße 98
   24103 Kiel
   Germany
   Tel +49-431-988-1200, Fax -1223
   http://www.datenschutzzentrum.de
   www.european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

Target of Evaluation is the product “SpeechMagic™ Solution Builder (Version 2.0)”.

The product supports digital dictation and contains a speech recognition system (SpeechMagic™), it supports a workflow that includes home-office typing and external typing offices as commonly used by hospitals.

The product, as a white label solution, is a software that is (or can be) implemented within a Hospital Information System. The ToE is not a stand-alone solution.

The ToE includes:

- The application.
- The data interface with a Hospital Information System.
- The data interface and software support of external workflows.

It does not include:

- Client hardware.
- Third party products (in particular SpeechMagic ™).
- Any part of the HIS (Hospital Informations System) software.
- Usage of the product via the internet.

7. General description of the IT product or IT-based service:

SpeechMagic™ Solution Builder is a software that is or can be implemented within a Hospital Information System (HIS) not a stand-alone-solution. SpeechMagic™ Solution Builder supports digital dictation. It collects recordings and dispatches them for manual transcription or automated speech recognition. The resulting documents are integrated in the patient’s data in the HIS. SpeecMagic Solution Builder contains a speech recognition system (SpeechMagic™) and supports an external workflow that includes home-office typing and external typing offices, as these are commonly used by hospitals. In this case, it is possible to pseudonymize audio files and transcriptions.

The dictations are saved to a central file server as encrypted audio files. Additionally, information may be stored in two data-fields: In the Patient field, any patient information can be entered, e.g. name and birth date, as a free text entry. The content of the patient field is not transferred to external typing offices. In the information field, additional information can be entered. This information will then be displayed in a special information field within the Report List and can be used by the transcriptionist as required. The information entered in this field contains free text. Any entries in these two fields are optional; they can also

be left empty. If the hospital has defined rules for the usage of these fields, it is strongly recommended to follow them.

The ToE includes the recording of dictations and the management of audio files as well as the data interface with the HIS. Support of external typing offices is also included. Usage of the product over the internet is not part of the TOE.

8. **Transnational issues:**

All data processing takes place within the network of the hospital. SpeechMagic™ Solution Builder focuses on customers in the European Union the software, however, is not geographically limited to EU customers.

9. **Tools used by the manufacturer of the IT product/provider of the IT-based service:**

Microsoft Visual Studio
Microsoft SQL Server

10. **Edition of EuroPriSe Criteria used for the evaluation:**

EuroPriSe Criteria Catalogue for Experts - Version 0.3

11. **Evaluation results:**

1. Documentation

The product is provided with comprehensive documentation, including information about privacy.
The processing of sensitive data, especially health related personal data usually requires specific additional organisational measures in order to ensure compliance with data protection law and, in particular, other specification regulation regarding the processing of health related data by doctors.
The documentation of the TOE supports controllers of data processing with very useful tips and information on additional organisational measures that may have to be applied or can be useful. Even though there may be specific legal requirements in some member states the information provided can be considered compliant in regard to the Data Protection Directive (95/46/EG). Therefore the support contained in the documentation can usually be applied by all controllers using the TOE.
In addition to the reference manuals for users and administrators there are configuration requirements and database installation guides.

All encryption methods are described in a document called “SMSB-Internals”. This applies to all technologies used with the product. It has to be kept in mind that the product is not a mass market product and depends on individual

implementation in a Hospital Information System. The core and privacy relevant elements remain untouched.

2. Technical Implementation (Encryption of Data)

Storing files on a central file server always includes the risk that these files are changed or accessed without authorisation. Therefore the manufacturer has implemented a technology which guarantees that only one “hidden user” has exclusive rights to change the data. This user runs as a service on an authorised workstation. This guarantees the data integrity. As a result, the dictations are saved on a file server and cannot be accessed by other users or programs. The information on these dictations is stored in a database.

Additionally the dictations are encrypted with a proprietary method.

3. Pseudonymization

Since the program can be used in connection with external typing offices, the data processing controller (e.g. the hospital) must ensure medical confidentiality. The manufacturer supports this with a pseudonymization function. All personal data (even the name of the doctor who created the report) are pseudonymized.

4. Processed Personal Data

The program is processing personal data of patients, which can be dictated by the medical doctor. In fact there is no need to do that. The synonym “the patient” can always be used.

Within a dictation, any kind of data can be recorded. If an MDIS (Medical Doctor Information System) is used, personal data will be transferred to SpeechMagic™ Solution Builder and will be displayed. At a minumum the name of the patient will be stored as dictation-related data.

5. Legal basis for processing of personal data

The TOE is always used within a medical environment, especially hospitals. Dictations that are done using the TOE usually contain special categories of data (e.g. health-related data) in the sense of Art. 8 (1) of the Directive 95/46/EC.

According to Art. 8 (3) of Directive 95/46/EC, Art. 8 (1) of Directive 95/46/EC will not apply where data processing is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

In the case of the TOE the usage scenario is restricted to hospitals and/or usage by doctors and the processing of health-related data.

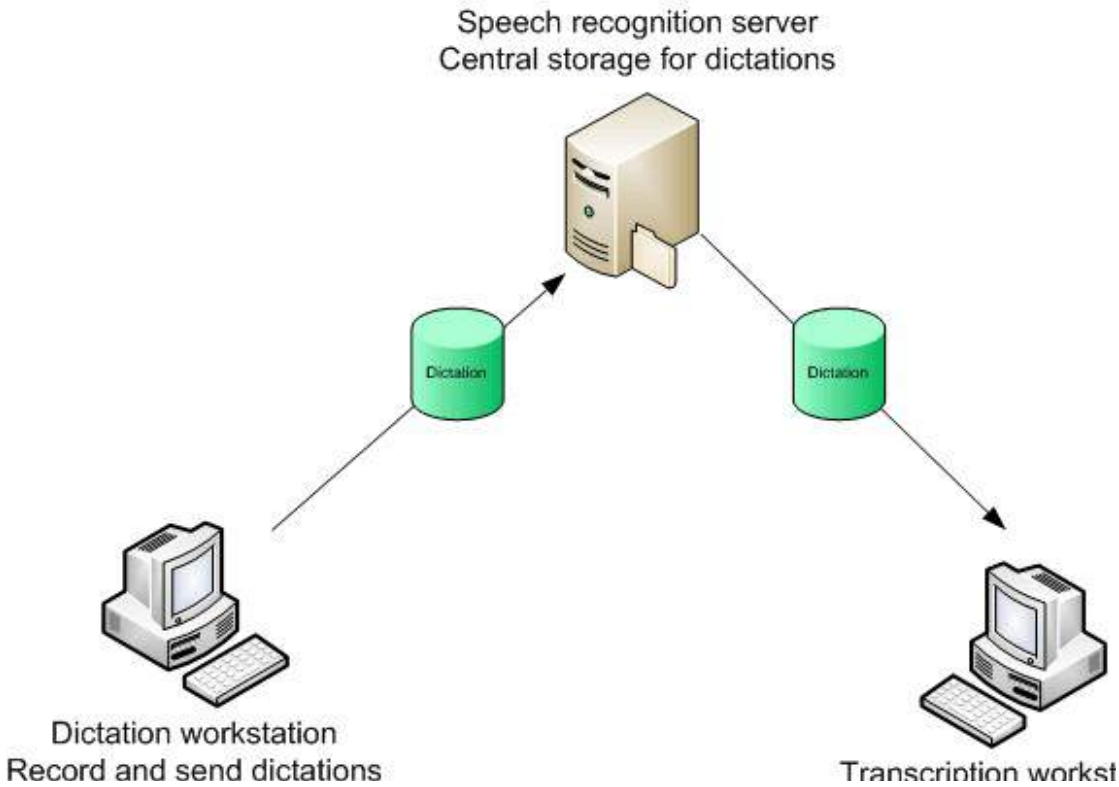
In most EU member states the processing of healthcare-related data is based on a medical treatment contract and/or consent of the patient.

Regularly, a patient signs a medical treatment contract when getting medical treatment in a hospital. In order to ensure the patient's therapy, it is necessary to document the patient record, etc. Many doctors dictate the patient information which is then written by typists. As the patient information is a serious contractual obligation by the doctor and/or hospital, the processing of personal data using the TOE can be considered as necessary for the performance of the contract pursuant to Art. 7 (b) of Directive 95/46/EC.

Furthermore the data processing of medical data of patients is lawful when the data subject has given their explicit consent (Art. 8(2)(a) of Directive 95/46/EC). The controller of the personal data processing often requests explicit consent by the data subject when the patient is taken to the hospital and signs the medical treatment contract or comparable documents.

The documentation of the TOE contains useful information regarding the legal requirements that may apply for the lawful processing of patient data and supports the controller to take the right measures in order to comply with Directive 95/46/EC.

12. **Data flow:**



13. **Privacy-enhancing functionality:**

The product successfully implements privacy-enhancing functionality with regard to data integrity and controlled data access; this is done via specific assignment of access rights to individual user groups

Policies concerning medical confidentiality (e.g. different levels of permissions that can be granted to individuals, departments or treatment teams) can be implemented in the product with the help of global and departmental guidelines.

In the case where external typing offices are used, the integrated technologies of pseudonymization will help to ensure compliance with privacy and medical confidentiality requirements.

14. **Issues demanding special user attention:**

If a connection with an external typing office is used, data pseudonymization can only be guaranteed if the medical doctor does not dictate the patient name. It is recommended to dictate "the patient" instead. The patient name can be associated with the report in the Patient field (which is not transferred to the external typing office).

This procedure is mandatory. Users should be aware that cooperation with external typing pools can constitute a breach of medical confidentiality which is

an offence that can be prosecuted under the national penal law of the European Union member states.

Implementing external typing offices by using the TOE can otherwise be lawful when the data subject (patient) has given their informed consent. Hospitals could e.g. include a special clause within the medical treatment contract.

In some member states the disclosure of medial data to third parties is unlawful or even punishable. In other member states or federal states specific legal regulation allows the disclosure of personal data of patients to third parties under specific circumstances.

The controller must take the necessary technical and organisational measures in order to comply with the relevant country legislation.

The documentation of the TOE provides useful advice in regard to taking the necessary measures to ensure maximum privacy.

For data pseudonymization to work properly, the program administrator must activate central the 'Anonymize data' mechanism.

15. **Compensation of weaknesses:**

Does not apply

16. **Decision table on relevant requirements:**

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	adequate	The manufacturer of the product has no influence on the recorded and processed data. When the product is used, the name of the patient should not be stored with each dictation. Rather a pseudonym e.g. a patient number should be used instead. Especially in dictations where any kind of data could be stored. This only refers to primary data. For secondary data the convention of data avoidance and minimisation are fulfilled with the aid of a 3-log-level staging concept, which is implemented for each SpeechMagic™ Solution Builder module and with a log rotation system.
Transparency	excellent	All encryption methods are described in a document called “SMSB-Internals”. The same applies to all technologies used with the product. It has to be kept in mind that the product is not a mass market product and depends on individual implementation in a Hospital Information System. The core and privacy relevant elements remain untouched. The manufacturer offers a very comprehensive user manual and a manual for administrators including information concerning privacy.
Technical-organisational Measures	adequate	The technical-organisational measures taken by SpeechMagic™ Solution Builder to ensure the protection of data are adequate. The encryption method for the

		recorded wave files is proprietary. All access files are encrypted with a standard 256 bit Rjindael algorithm.
Data Subjects' Rights	adequate	Regarding the primary data of ToE users (doctors), there is sufficient information provided to the data subjects about the processing of their personal data. The product documentation and the product interface itself are transparent with regard to the data processing carried out with the product. With regard to patient data it should be mentioned that the patients are regularly informed about the processing of data for medical purposes. There is no further information by the controller needed when using the ToE.

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.

Flensburg, 26.05.2010	Stephan Hansen-Oest	
Place, date	Name of Legal Expert	Signature of Legal Expert

Kellinghusen, 26.05.2010	Andreas Bethke	
Place, date	Name of Technical Expert	Signature of Technical Expert

Certification 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 security.

Place, date	Name of Certification Body	Signature