



Speech Machines Limited

Data Protection Act 1998 compliance

Speech Machines Limited is registered under the Data Protection Act as Number Z5577059.

In respect of the Document Enterprise Platform, Speech Machines is a “Data Processor” as defined by the Act. The Act does not provide for registration of Data Processors, but does impose duties and responsibilities which are expressed in eight principles. Speech Machines, MedQuist, and Philips take these responsibilities seriously and have taken all reasonable measures to ensure compliance.

Data Protection Act Detailed Compliance

The Data Protection Act 1998 contains eight principles as follows:

1. To process personal data fairly and lawfully
2. To process personal data only for specified purposes
3. To ensure that personal data is adequate, relevant, and not excessive
4. To ensure that personal data is accurate and up to date
5. To ensure that personal data is kept for no longer than necessary
6. To process personal data in accordance with the rights of the individual
7. To process data in a secure environment
8. Not to transfer personal data to a country that does not offer an adequate level of protection to the individual

Speech Machines is a Data Processor and responsible for compliance with items 1,2,6,7,8 above. Items 3,4,5 are the responsibility of the Data Controller, ie our clients. In the case of item 5 Speech Machines is responsible for implementing the data retention period specified in writing by each client.

Data Protection Act first and second principles (data processing):-

The Service Agreement signed by each client specifically commits Speech Machines to meet the requirements in the first and second principle listed above, namely to process data fairly, lawfully, and only for specified purposes.

In order to comply with its responsibilities under principles 5, 6, 7 and 8 Speech Machines has taken the following measures:-

Data Protection Act fifth principle (data retention):-

Speech Machines DEP system needs to store individual dictations while they are in the process of being typed. This includes work queued for automatic speech recognition, typing, and finished work being formatted and returned to the client.

Voice files are deleted shortly after a job is finished and returned to the client.

The length of time for which copies of documents are retained is configurable for each type of work, and for each client. Clients often require us to retain copies of their documents for many years, for example the UK Inland Revenue and H. M. Customs & Excise require that financial documents are retained for six years, we therefore provide this facility to UK financial institutions.

Speech Machines data archive servers provide greater confidentiality and resilience than almost all other methods of electronic file storage, therefore many clients choose to use us as a data storage resource.



Some NHS Trusts require documents to only be stored within NHS premises. Therefore, Speech Machines undertakes to delete documents from the DEP when they have been successfully returned to the hospital server.

Data Protection Act sixth principle (individual rights):-

Individual dictations are not subject to operator intervention as all processing by Speech Machines Ltd is automatic; therefore the rights of any individual data subject are not compromised by using the DEP system.

The only circumstances when a dictation or document might be accessed is in the event of a technical failure, or a client request for assistance, in which case only the minimum amount of personal information would be accessed, and only by authorised Speech Machines or Medquist Technical Support or Customer Support employees. The DEP processes more than 50,000 documents per day so regular manual intervention is not feasible.

Every Speech Machines and MedQuist employee is required to sign an extensive confidentiality agreement as part of their Contract of Employment. A copy is attached to this document.

Data Protection Act seventh principle (secure environment):-

Secure transmission of data:-

Security during the transmission of data is just as important as where the processing takes place, Speech Machines DEP system transfers data as follows:-

- transfer of dictation voice files to data centre
- transfer of dictation files to typists
- transfer of typed work back to the data centre
- transfer of finished document to client for archive or storage

In all data transfer circumstances Speech Machines employs the highest industry standard security measures, and utilises the same technology as internet banking transactions:-

- Secure Socket Layer (SSL) connection for all communication to ensure no unauthorised interception of files can take place
- Data transferred encrypted to 128bit standard
- User name, password, and company id number, validated against the main database in order to commence every communication session

Secure processing environment

The processing equipment is located in two hardened data centres owned and managed by Sungard Inc, the leading provider of secure processing centres in the US

<http://www.availability.sungard.com/>

Sungard facilities include:

- 24x7 security guards
- No access to the building to unauthorised personnel
- Access to individual data suites only available to named individuals who are pre-booked by appointment
- Power backup from battery supplies and independent generators
- Multiple internet and telephone connections
- Firewall protection using latest software to prevent unauthorised remote access to data centre servers
- Anti virus software updated daily to protect data from attack by foreign programs
- On-site technical support 24x7



Data Protection Act eighth principle:-

“Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data”

The European Union Commission has negotiated a set of rules called “Safe Harbor” principles with the US Department of Commerce that enables data to be sent to the USA for processing provided the US Data Receiver demonstrates commitment to these principles. Speech Machines has therefore entered into a “Safe Harbor” Agreement with MedQuist Inc – a copy of which is available on request.

Schedule 1

Speech Machines Limited extract from Employment Contract:

“Employee Confidentiality statement

I understand, that as part of my employment by Speech Machines, I may be granted access to patient health information or confidential financial information. In consideration of and as a condition to my employment, I agree that all information, including but not limited to, any patient health information, that I obtain or come into contact with during my employment with Speech Machines is strictly confidential. I understand that for purposes of this agreement Confidential Information includes, but is not limited to, all patient health information, personal financial information, computer passwords, software, proprietary information, trade secrets, employee and worker lists, client information and trade information regarding or about Speech Machines business practices and/or transactions. I also agree that any disclosures or unauthorised use of and/or unauthorised access to Confidential Information will be grounds for immediate termination of my employment with Speech Machines. With respect to Confidential Information, I agree:

I will use Confidential Information for the sole purpose of performing the duties and responsibilities Speech Machines has engaged me to perform.

I will not disclose or discuss any Confidential Information to or with any person whatsoever who is not a representative of Speech Machines (i.e. spouses, friends, family and acquaintances) or to or with any representative of Speech Machines who does not have a legitimate right to know. Without limiting the generality of the foregoing, I will not disclose, discuss, reproduce, copy, forward, e-mail, mail, duplicate, copy, disseminate or remove any patient health information except to the extent it is required to perform my duties and responsibilities for Speech Machines and only so long as it is otherwise permitted under the terms of this Agreement. I understand this applies to both hard copies and electronic (computer) copies of information.

I will use appropriate safeguards to prevent the use or disclosure of the Confidential Information other than as provided for by this Agreement.

I will comply strictly with all Speech Machines Policies on Confidentiality and Information Security.



I will complete all awareness, education and training requirements on privacy and security programs.

I will report immediately to Speech Machines any violation of the terms of this Agreement or unauthorized use, duplication, disclosure, or dissemination of Confidential Information by any person, including myself.

Upon the termination of my employment, I will immediately destroy or return to Speech Machines any documents or any other media (hardcopy or electronic) containing any Confidential Information and will certify that in writing to Speech Machines.

I agree to indemnify Speech Machines fully for any and all damages, including legal fees, Speech Machines may incur as a result of my breach of this Agreement.

I agree that all my obligations under this Confidentiality Agreement shall survive termination of my employment by Speech Machines regardless of the reason for termination.”