SACHVERSTÄNDIGEN-BÜRO FÜR COMPUTERWESEN
PROF. DR. PAUSCH & PARTNER

Office Darmstadt: D-64289 Darmstadt, Heinheimer Strasse 38
Tel: +49-6151/9712640 Fax: +49-6151/9712641
Office Kassel: D-34277 Fuldabrück, An der Röthe 10
Tel: +49-561/95339100 Fax: +49-561/95339101
Office Grünstadt: D-67310 Hettenleidelheim, Im Park 9
Tel: +49-6351/1359000 Fax: +49-6351/1359001
Office Pegnitz: D-91257 Pegnitz, Reisach 16
Tel: +49-9241/7359000 Fax: +49-9241/7359001
Office Sydney: Level 6, 8 Spring Street, Sydney 2000, NSW, Australia
Tel: +61-2 8296 04 92 Fax +61-2 8296 04 11

Report 150330/04
Data privacy Audit

On behalf of

Newleaf Partners Europe GmbH
Rotdornweg 5
D-63303 Dreieich-Buchschlag

Dipl.-Ing. Mathias Gärtner
von der Industrie- und Handelskammer Darmstadt
öffentlich bestellter und vereidigter Sachverständiger
für das Sachgebiet Systeme und Anwendungen
der Informationsverarbeitung für den Bereich Netzwerktechnik

COPYRIGHT © 2015, Dipl.-Ing. M. Gärtner
This report is protected by copyright of the author. It may contain personal data as defined in the german data privacy act (BDSG). The report may only be used for the intended purpose. Any reproduction, in whole or partial by any means is subject of the author's permit.

Data privacy:

Every data required for preparing and writing this report is stored by electronic means and will only be used for this report. The data is not given to third parties unless a specific law requires.

1.Scope of work

I was given the task to prepare a data privacy audit of the procedures and IT-programs used in the company New Leafs Partners Europe GmbH according to the standards set forth in the german privacy law BDSG, namely article §9.
I was contracted because of my qualifications as data privacy officer and as a publicly certified expert witness for Information Technology.

2.Summary

I have done an audit of the technical and organizational measures on the data processing hard- and software of NewLeaf Partners Europe GmbH.
The personal data that is being collected and processed is not very sensitive data. It consists mainly out of the names and the non-private e-mail address of a person that is enrolled in online learning with the Q-software of NewLeaf Partners Europe GmbH.

All measures are up-to-date with the current technical standards and are suitable for the type of data that is being processed.

The server itself is hosted in a computing center with a very high security standard (ISO 27001 and PCI DSS L1).

All required organizational methods and contracts are in force.

The hard- and software and the organization for personal data processing at NewLeaf Partners Europe GmbH can be considered secure and according the required standards.

3.Required procedures as defined by law

The legal framework for gathering, storing and processing of private data is defined by the german data privacy law (BDSG). The current version was put into action by Sept. 1st of 2009.
According this law, the gathering, storing and processing of private data is only possible under the exceptions set fort in §4. All data that can be defined as
“Specific information that describe the identity of a person or contains information that describe specific situations of a person” (§3, Abs I BDSG) are protected under that law.
The law does explicitly not limit the data processing to actual or possible breaches of privacy or individual laws of a person but uses a very broad definition. There is no explicit definition of private data, however, every

piece of data that can directly or indirectly be linked to one person, can be considered as private data.
The law defines in §9 BDSG all the required technical and organizational procedures in order to be allowed to process personal data.

The law further defines penalties for breeching any of the defined procedures.
The report will check the data processing situation of the NewLeaf Partners Europe GmbH against these set of procedures.

4. Methodology

In order to prepare for this report, I conducted a workshop on July 2nd of 2014 with the CEO of NewLeaf Partners Europe GmbH, a Mr. Goldmann and the responsible IT person, a Mrs. Heidt.

Duringthe workshop the following information were presented and form the basis of this report:

- The type of data that is collected, stored and processed, i.e. names, addresses or work descriptions
- The IT-systems (hard- and software) used to collect, store and process that data
- Procedures used to collect, store, process and delete data

On Aug 6 2014, the IT system and specificity the program named “Q” in use was examined by myself in order to find specific information of how this program is processing private data. It was explicitly checked for the features

- the possible use of mandates so that one mandate may not see the data of another
- possible separation of data delivered by individual customers and
- general data security

5. Results

5.1. Definitions

Personal data. This data is information about the personal or factual situation of a specific person or of persons who can be identified by little effort.

Data processing is the act of using personal data in form of gathering, storing or processing.

Gathering is the process of obtaining personal data either by actively asking or by receiving data from third parties (ie. Customers).

Storing is receiving and storing personal data onto any kind of storage device for further processing.

Transmitting is the process of copying obtained and stored personal data to third parties either by actively sending the data or by presenting the data so that the third party may download or copy the data.

Locking is a process to mark personal data unsuitable for further processing of any kind (this also includes transmitting).

Deleting is the process of removing personal data from the storage or to make the data anonymised so that the individual person cannot be identified anymore.

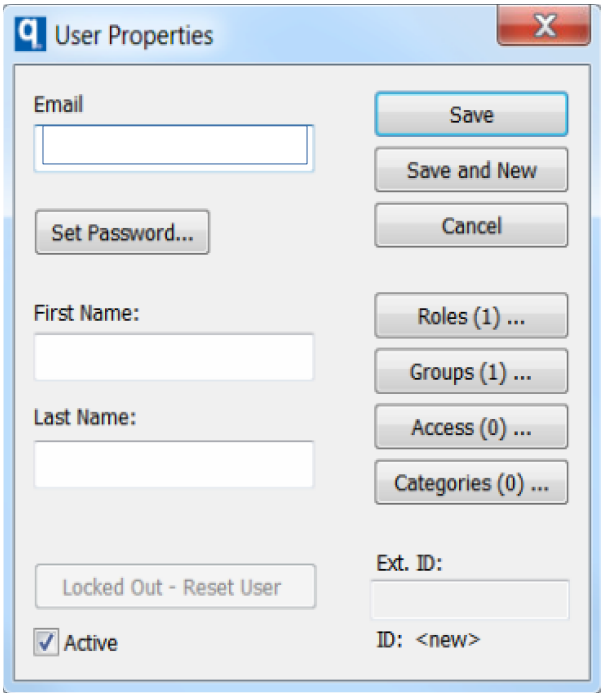
Dataprocessing entity is the legal or biological person that is gathering, storing or processing the personal data.
Third party is any legal or biological person that is receiving personal data for their own usage (not to confuse with a party that is receiving the data in order to process them on behalf of the dataprocessing entity).

5.2. Personal data processed by NewLeaf Partners Europe GmbH

The companies service is to provide online learning facilities. This includes the presentation of the learning material as well as the administration of the individual learning progress.
In order to be able to provide that service the following data must be collected on behalf of the individual trying to learn.

- Given and surname of the learner and
- the e-mail address of the learner. This data is not required but should be given to be able to receive individual progress reports.

No additional data is obtained.
There is no requirement that the names provided must be real names. They may be pseudonyms. The name is only used to individually identify the learning person in oder to collect his/her progress.



Picture 1: Data input form

As seen in picture 1 the administrator may assign specific roles to the user. This data is only used for internal processing and has no personal meaning towards the user. The roles may be used to permit or deny specific learning topics for that user.

The mentioned data is given to NewLeaf Partners Europe GmbH by companies who wish to have their employees trained. That implies that the sending company is responsible for obtaining the required permits in order to be able to send the personal data towards NewLeaf.

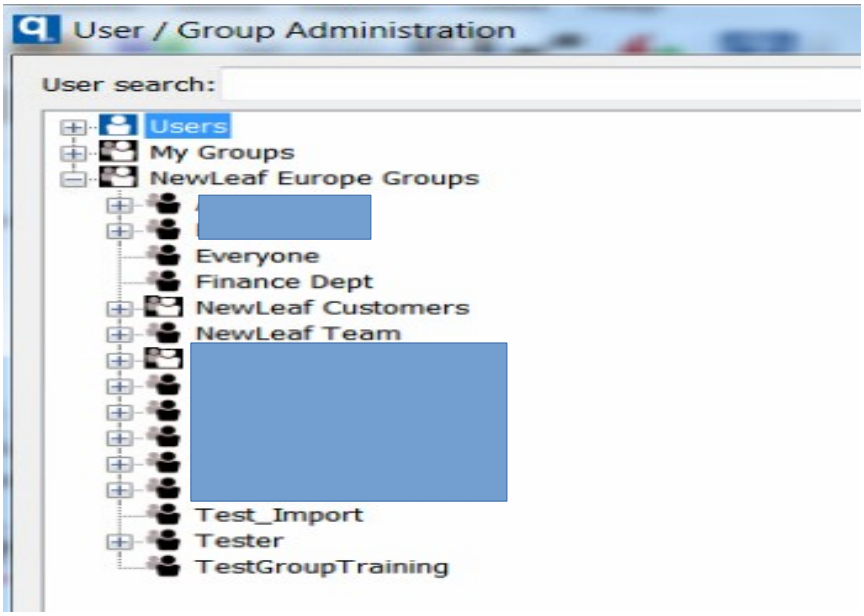
5.3. Technical processing

The personal data is delivered to NewLeaf Partners Europe GmbH by e-mail. The e-mail contains an Excel file which contains the required data. This data then is imported into the “Q” program. This task is performed by a subcontractor who is legally bound to data privacy according to §11 BDSG.

Picture 2: Typical excel data sheet received by customers of Newleaf

There is one special user in the program, the so called “superuser”. Only this user has full access to all the data imported into the system. This super user role is currently assigned to the subcontractor as an individual person only.

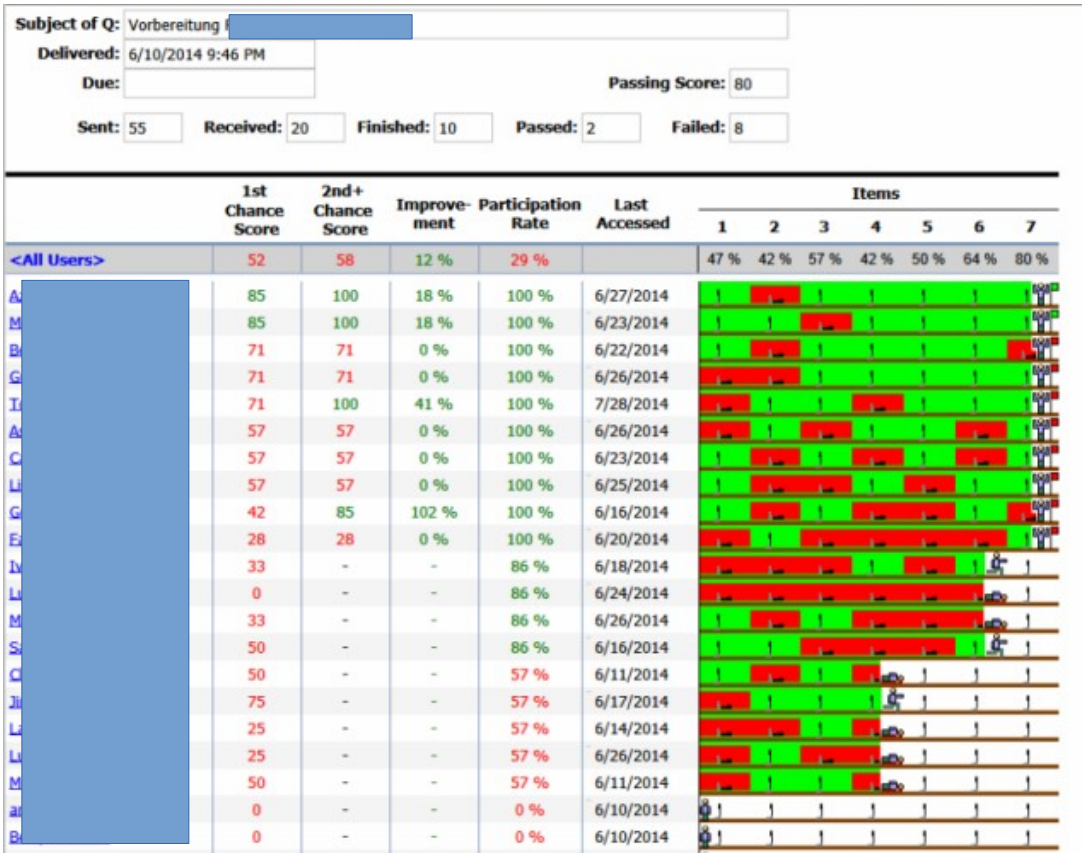
The software knows about a role as “mandate-admin”. These users do only have access to the data of the defined mandate. Other users do only have access to their own data.



Picture 3: Accessible groups for the superuser

The mandate administrator may create reports of the progress of the individual learners in his group and may send them to either the individual (e-

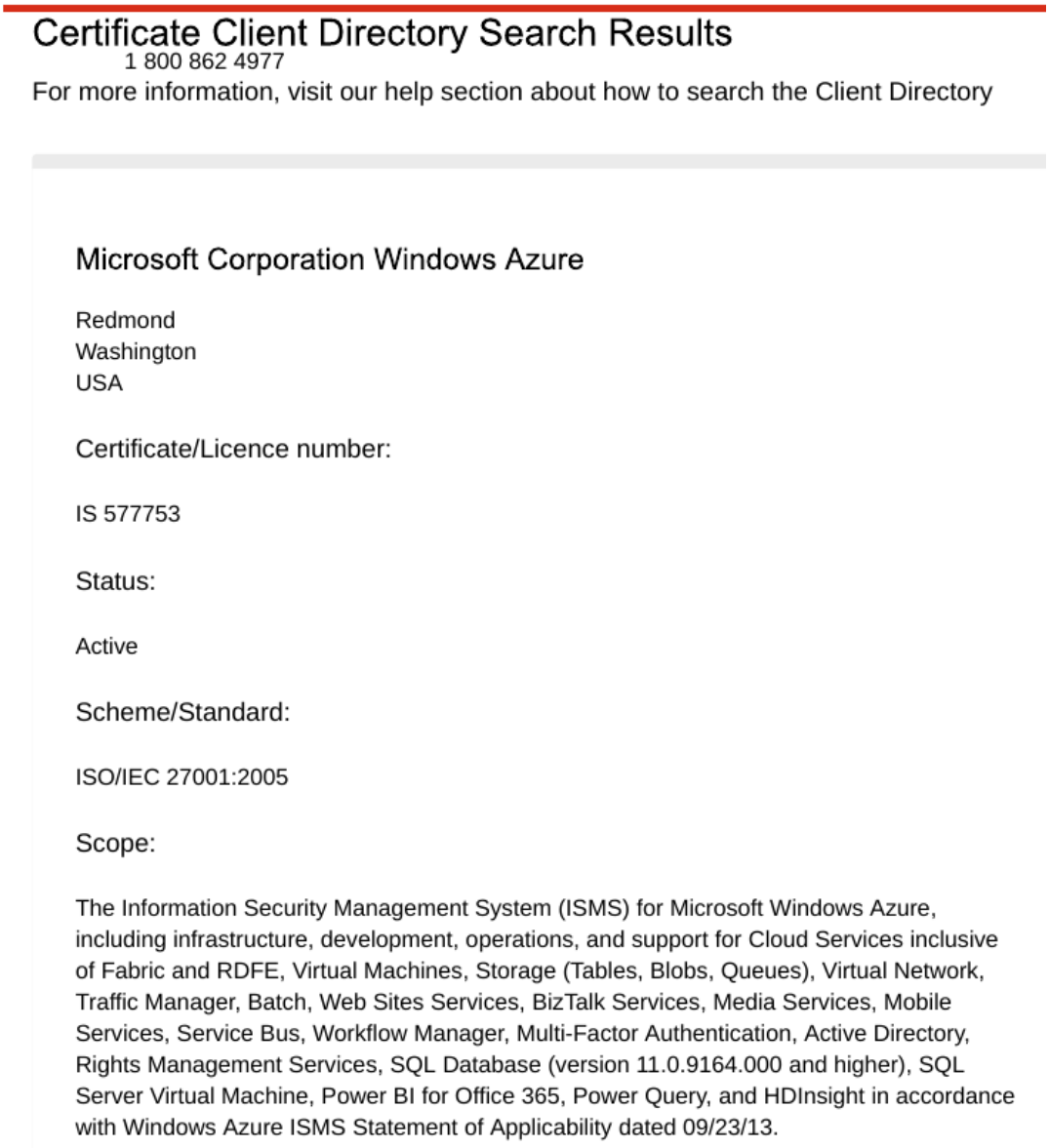
mail address must be provided) or to the customer who entered these individuals to the course.
The report generation is manual, no automatic generation is possible.
The report shows the individual progress of a leaner in the course as seen in picture 4. As there is no automatism, sending this data to the wrong persons is only possible by explicit admin error.



Picture 4: Sample report of one lecture

5.4. Technical security of the data processing system

The required procedures and technical measures to secure the data processing system when processing personal data is described in §9 BDSG and it's appendix.
I found that the server with the software “Q”, the actual lecturing software, is hosted in the Microsoft Azure computing center in Amsterdam. Microsoft provides an up-to-date certificate with a successful ISO 27001 audit (see picture 5). In addition to that Microsoft did provide with an up-to-date PCI-DSS Level 1 certificate. This is sufficient to prove that the physical and technical security is excellent.
The administration of the server (OS and the Q software) is done by the american mother company. The administrators are bound by contract to regard the required data privacy rules.



Certificate Client Directory Search Results

1 800 862 4977

For more information, visit our help section about how to search the Client Directory

Microsoft Corporation Windows Azure

Redmond
Washington
USA

Certificate/Licence number:

IS 577753

Status:

Active

Scheme/Standard:

ISO/IEC 27001:2005

Scope:

The Information Security Management System (ISMS) for Microsoft Windows Azure, including infrastructure, development, operations, and support for Cloud Services inclusive of Fabric and RDFE, Virtual Machines, Storage (Tables, Blobs, Queues), Virtual Network, Traffic Manager, Batch, Web Sites Services, BizTalk Services, Media Services, Mobile Services, Service Bus, Workflow Manager, Multi-Factor Authentication, Active Directory, Rights Management Services, SQL Database (version 11.0.9164.000 and higher), SQL Server Virtual Machine, Power BI for Office 365, Power Query, and HDInsight in accordance with Windows Azure ISMS Statement of Applicability dated 09/23/13.

Picture 5: ISO27001-Certificate of Microsoft Azure

In total this ensures that the technical system, including physical infrastructure, server software and administrator accesses is fulfilling the standard set forth by law.

5

5.5. Organizational security

The general organization can be described as very small. In total two persons are involved with the processing of personal data. The CEO is responsible for administering the personal data needed to fulfill the contracts, i.e. invoice addresses. All other personal data is handled by the subcontractor which is bound by contract to oblige the required data protection rules. A suitable contract was presented to me.

Since the data is received by means of e-mail (the excel file is an attachment) I recommended to use password protected Excel files. While this is not the most secure method it will provide sufficient data protection for the type of personal data transported this way.

After importing the Excel file data into the Q system, the e-mail and the Excel file itself are deleted on the system of the subcontractor.

5.6. Register of processing operations

Both required registers of processing operations were presented to me and describe the processing operations for personal data.

5.7. Data privacy officer

At the time of this audit, no data privacy officer was employed. However, this is not a requirement by law since this is usually only required if nine or more persons are working with personal data.

5.8. Transmission of personal data to third parties

There is no transmission of personal data to any third party of any kind.

6. Final declaration

I hereby declare that I created this report without any interference by others. Also this report was created without the preference of any party involved and without any financial interest in the products reported.
I hereby confirm that a have created this report under the obligations of the public oath given by me on Mar 2000 in order to become a publicly certified IT expert witness.

Darmstadt, the 22nd of April 2015

Dipl.-Ing. Mathias Gärtner
von der Industrie- und Handelskammer Darmstadt
öffentlich bestellter und vereidigter Sachverständiger
für das Sachgebiet Systeme und Anwendungen
der Informationsverarbeitung für den Bereich Netzwerktechnik

Dokument unterschrieben
von: Mathias Gärtner
am: 23.04.2015 16:45
Ort: Darmstadt
signierte Gutachtenkopie