Short Public Report

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

   PseudoDat – function as provided in January 2011

2. Provider of the IT-based service:

   Company Name: m-privacy GmbH

   Address: Am Köllnischen Park 1
   10179 Berlin

   Contact Person:Holger Maczkowsky

3. Time frame of evaluation:

   October 23rd 2009 – March 21st 2011

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

   Name of the Legal Expert: Stephan Hansen-Oest

   Address of the Legal Expert: Neustadt 56
   24939 Flensburg
   Germany

Name of the Technical Expert:	Andreas Bethke
Address of the Technical Expert:	Papenbergallee 34 25548 Kellinghusen Germany

5. Certification Body:

Name:	Unabhaengiges Landeszentrum fuer Datenschutz - ULD
Address:	Holstenstr. 98 24103 Kiel Germany
eMail:	europrise@datenschutzzentrum.de

6. Specification of Target of Evaluation (ToE):

ToE is the IT service PseudoDat by the German „m-privacy GmbH".

PseudoDat is a service offering users enhanced possibilities of matching their own address data pools with address data pools of an address data provider in the case of buying or renting address data. PseudoDat is thereby supposed to help avoiding duplicate copies of address data.

PseudoDat offers a privacy friendly way to match address data pools by enabling a comparison of separate address data pools based on pseudonymized data. Neither the provider of address data nor the customer that wants to buy address data from the address provider have access to personal identifiable data by the other party. Furthermore, m-privacy GmbH doesn't have access to these pools either.

The service consists of several IT-systems that are provided to the address data provider and address data customer by the m-privacy GmbH. The IT-systems are a combination of hard- and software that is specifically produced for carrying out the comparison procedures of address data pools.

There are always three parties involved in every comparison of address data pools using the ToE:

1. Address Data Provider:
   The address data provider uses the IT-system "PseudoDat Provider"
2. Address Data Customer:
   The customer of address data uses the IT-system "PseudoDat Customer"
3. m-privacy GmbH:
   The m-privacy GmbH does provide the "PseudoDat Rendezvous Server" which

does provide the key management and services of comparing pseudonymized data.

Components of the ToE are:

- PseudoDat-Rendezvous-Server
- Applications needed to run „PseudoDat Provider“
- Applications needed to run „PseudoDat Customer (Kunde)“
- Public-Key-Management on „PseudoDat Rendezvous Server“
- VPN-secured connection of the systems „PseudoDat Provider“ and „PseudoDat Customer (Kunde)“

The following components are not part of the ToE:

- Billing & payment of services that have been conducted using the ToE
- Operating systems used to run the applications on the PseudoDat systems
- Technical support by m-privacy GmbH

7. General description of the IT-based service:

PseudoDat enables the comparison of several address data pools of an address data provider and address data customer without the disclosure of personal identifiable information.

The service can be described best by using a practical example:

Imagine company „X“ wants to send out a direct mailing to 10.000 households. Company „X“ may not just want to use their own address data but buy further address data by an address data provider. In order to avoid duplicate sendings to households company “X” wants to compare the address data that it wants to buy with their own address data in order to check for duplicates. This is a common practice in the field of the selling (or renting) of address data.

In order to conduct the comparison of address data the customer of address data would have to send their own address data to the address data provider or vice versa. This commonly leads to a disclosure of personal data to the other party conducting the address data comparison. Due to a usually not existing consent of the data subject the disclosure of personal data may be unlawful.

PseudoDat has been developed to solve the potential data protection issues of comparing several address data pools when buying (or renting) address data from address data providers.

The procedure of comparing data in address data pools between customer and provider of address data when using the PseudoDat is as follows:

The customer of address data – company "X" uses the system "PseudoDat Customer (Kunde)" that is provided by the m-privacy GmbH – either as an appliance or run as a virtual machine (like VMware). PseudoDat Customer (Kunde) is an application that runs on the TightGate Server Solution – a specially hardened operating system that has been developed by m-privacy GmbH.

The provider of address data uses the system "PseudoDat Provider" that is likewise provided by the m-privacy GmbH. It is equally based on the Tight-Gate Server Solution.

Both systems – PseudoDat Provider and PseudoDat Customer (Kunde) - connect with the "PseudoDat Rendezvous Server" that is maintained and managed by m-privacy GmbH. PseudoDat Rendezvous Server is based on the FreeBSD operating system.

To initiate an address data comparison procedure company "X" will have to save an address data file (e.g. a .csv file) on their local PseudoDat Customer (Kunde) installation. It would then have to choose a comparison/matching procedure that are usually individually implemented by m-privacy for the client in advance.

The address data will be pseudonymized by the use of hash values within the PseudoDat Customer (Kunde) system and is then sent to the PseudoDat Rendezvous Server through a VPN-tunnel. The pseudonymized and encrypted address data is stored on the PseudoDat Rendezvous server for the purpose of matching. m-privacy GmbH does not have access to any personal identifiable address data and is not able to decrypt or de-pseudonymize address data.

The address data provider will see that new data for comparing has been sent by company "X" to the PseudoDat Rendezvous Server within his PseudoDat Provider system.

It's important to stress that address data of company "X" is not sent or disclosed to the address data provider. The address data provider will only receive a pseudonymization key that is necessary for submitting his own address data to the PseudoDat Rendezvous Server.

The provider of address data will save his address data equally as a file in his PseudoDat Provider system. The PseudoDat Provider system will pseudonymize the address data using the submitted pseudonymization key. The address data provider will then upload his data to the PseudoDat Rendezvous Server via a VPN-tunnel.

The matching/comparison procedure for checking of duplicates is completely run on the PseudoDat Rendezvous Server system. The checking routine is based on hashcodes. The results of the comparison procedure is sent to both parties – PseudoDat Consumer (Kunde) and PseudoDat provider – in an assembled list that contains just sums of checked data sets etc. but no personal data.

The m-privacy GmbH offers the implementation of further detailed reports on an individual by project basis.

Based on the matching report the address provider can then provide the suitable address data that can be bought (or rented) by the customer (company "X").

The pseudonymized address data sets are stored in the PseudoDat Rendezvous Server for 90 days.

8. Transnational issues:

   The service is offered in Germany and principally in any other member state of the European Union or the European Economic Area (EEA). Core target market is Germany at the time.

   There are no transnational issues with using the product. A transmission of personal data to third countries is not implied.

9. Tools used by the provider of the IT-based service:

   - GCC 4.2/4.3
   - Apache 2.2
   - Python 2.5
   - PHP 5.2
   - CakePHP 1.3
   - postgresql 8.3
   - OpenSSH 5.1
   - TightGate (a special "hardened" Linux based OS developed by m-privacy GmbH)
   - FreeBSD

10. Edition of EuroPriSe Criteria used for the evaluation:

    EuroPriSe Criteria 1.0 (May 2010)

11. Evaluation results:

Legal Evaluation

The ToE is mainly used in an environment of the buying and selling of address data for advertising purposes. The processing of personal data for advertising purposes is – even though Directive 95/46/EC does not include specific rules – object to legal regulation in some member states. Especially in Germany the processing of personal data for advertising purposes usually has to be based on consent of the data subject.

The operator of the PseudoDat service – m-privacy GmbH – has to rely on the responsible and lawful usage of their service by the providers and customers of address data using the PseudoDat service, who qualify as controllers in the sense of Article 2(d) of Directive 95/46/EC. They are responsible to process only data of data subjects that have given their consent for the processing of their data for advertising purposes.

In order to support the lawful usage of the ToE m-privacy GmbH provides a comprehensive documentation of the product and services for the users. Besides technical details m-privacy GmbH offers written advice for the data protection compliant use of the product and services.

As address data is stored encrypted within the PseudoDat Rendezvous Server system m-privacy GmbH has no access to address data of providers or customers.

For provisioning of their services m-privacy does have access to the following data of their clients:

- account data (username, password)
- email address (for notification purposes)
- log files (including account data, timestamps)

m-privacy GmbH advises their clients to choose non personal identifiable data for account data and email addresses. Nevertheless m-privacy can not grant that these data can be personal identifiable information. The processing of these data can be based on performance of the contract and is permitted for all data concerned.

Implementation and realization of data subject rights can be evaluated as adequate. As m-privacy does not have access to any address data, except account data and email address data of their own clients, there are no special measures in place for enhancing a special privacy friendly way concerning data subject rights.

Technical evaluation

m-privacy GmbH as operator of the PseudoDat Rendezvous Server has taken sufficient physical access control measures in order to prevent third parties from gaining access to personal data. These measures are documented in an IT security concept and can be evaluated as adequate.

Furthermore m-privacy GmbH has implemented excellent technical measures regarding the prevention of access to data, programs and devices. A very well thought-out authorization system, specific password rules provide good protection against unauthorized access by third parties.

Failed login attempts are recorded in log files and in case of multiple failed login attempts access will be blocked temporarily.

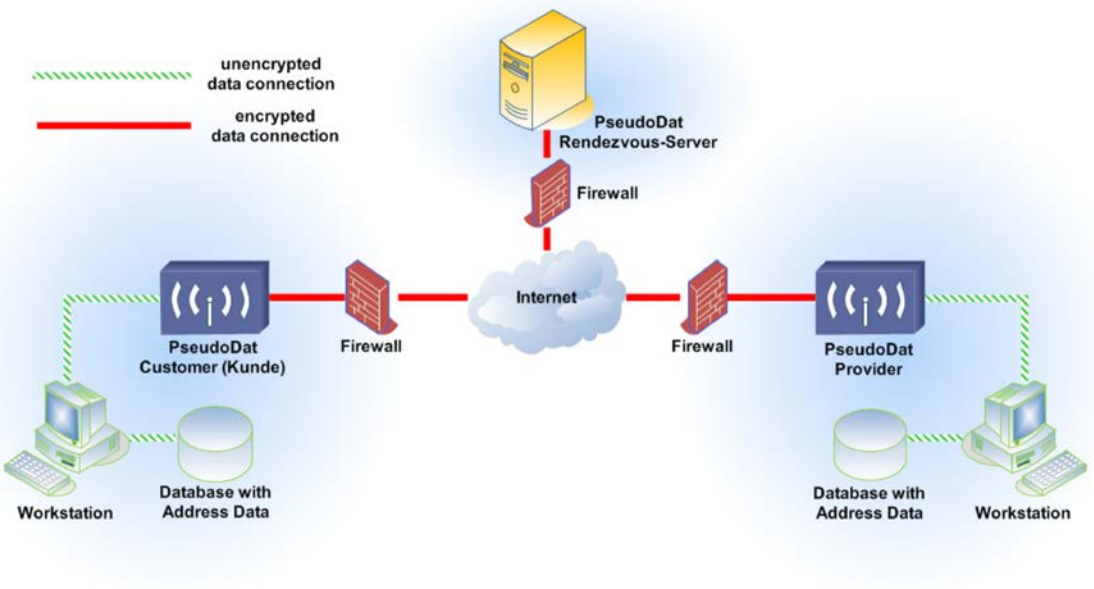
The logging mechanisms in place can be evaluated as excellent as log files are kept just to the necessary extent.

m-privacy GmbH has secured all network- and communication connections by using VPN tunnel technology. The encryption algorithm for the VPN tunnel corresponds to state-of-the-art technology.

The encryption and pseudonymization procedures used within the ToE can be evaluated as excellent. The encryption of the pseudonymisation key is based on the public-key cryptography based on GnuPG using the encryption algorithms DSA and ElGamal. m-privacy takes care of using sufficient key length that protects all personal data from unauthorized access by third parties. The used key length of 4096 bit and 1024 bit does ensure sufficient protection of concerned data.

The general data protection and security management measures taken by m-privacy GmbH can be evaluated as adequate.

12. Data flow:



13. Privacy-enhancing functionalities:

PseudoDat does provide significant privacy enhancing functionalities in an area that is often known to be very "data intense". By the use of state of the art encryption technologies m-privacy GmbH does provide possibilities to conduct the necessary matching/comparison procedures to avoid duplicate data when buying (or renting) address data from an address data provider.

The core functionality of checking for duplicate content is conducted without processing any personal identifiable information using hash codes and pseudonymization.

m-privacy GmbH does not have access to personal address data from the address pools. Furthermore, each address pool subject to matching/comparison is protected and address data is not disclosed to the other party involved in the matching/comparison routine. On the service level, m-privacy advises customers to the service to not include any personal data for account data (username) and email address . This – in fact – can not always be avoided when using the ToE.

14. Issues demanding special user attention:

Does not apply.

15. Compensation of weaknesses:

Does not apply.

16. Decision table on relevant requirements:

EuroPriSe Requirement	Decision	Remarks
Data Avoidance and Minimisation	excellent	With PseudoDat m-privacy GmbH does provide significant privacy friendly features by intelligent use of pseudonymization and encryption technologies. The core functionalities for comparison/matching procedures of address data pools are conducted without any personal identifiable information.
Transparency	excellent	m-privacy GmbH does provide a comprehensive documentation of the product and services and the technical details for pseudonymization and encryption. Furthermore suggestions for a data protection friendly implementation and use of the ToE are included in the documentation.
Technical-Organisational Measures	adequate	m-privacy has taken sufficient measures to prevent unauthorized access to data, programs, premises and devices that are evaluated as adequate. The logging mechanisms regarding the processing of personal data are evaluated as excellent. The transmission of data between the several PseudoDat systems is conducted completely encrypted via a VPN tunnel and is evaluated as excellent. The taken measures to prevent

		accidental loss of data are evaluated as adequate. The data protection and security management and the disposal and erasure of data are also evaluated as adequate. The technology-specific and service-specific requirements (encryption and pseudonymization/ anonymization) are evaluated as excellent. Altogether, the technical-organizational measures are evaluated as adequate
Data Subjects' Rights	adequate	Implementation and realization of data subject rights is evaluated as adequate. An excellent evaluation could not be conferred as there are no special measures in place for enhancing a special privacy friendly way concerning data subject rights.

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.

Flensburg, 11.04.2011	Stephan Hansen-Oest	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Kellinghusen, 10.04.2011	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-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 Body	Signature