Short Public Report

DiaDirekt is offered to customers around the world as a service to get their photo negatives, APS and slides professionally transferred to digital media at a low price, without any unexpected add-on costs or unclear terms.

The expert has evaluated if DiaDirekt meets all the requirements set out by the applicable data protection and data security laws and regulations. The service includes not only the handling of customers' personal data, but the images themselves can also be considered personal data, e.g. portraits.

DiaDirekt service ensures privacy by using several data minimization techniques:

- All mandatory handling of personal information is to fulfil the service obligations to the customers and to perform business planning.
- Communication and marketing letters via e-mail is optional and always based on the choice of the customer.
- The company never sells, leases or publishes data to third parties unless approved by the customer.
- Images stored at the premises are securely destroyed after the service has been performed.

In conclusion the expert finds that DiaDirekt is designed to facilitate the processing of personal data in a manner compliant to European regulations on data protection and data security. There is no personal data collected secretly or surprisingly. DiaDirekt fulfills all the requirements.

1. Name of the IT-based service:

   The service as provided on November 7, 2008, under the name DiaDirekt.

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

   Company Name: Tsevnic KB

   Address: Förbindelsevägen 7, SE-429 30 Kullavik, Sweden

   Contact Person: Malin Abrahamsson

3. Time frame of evaluation:

   2008-02-01 – 2008-11-07

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

   Name of the Legal and Technical Expert: Johan Dahlsjö

   Address: Foyen Advokatfirma AB, Kungsgatan 18, SE-411 19 Göteborg, Sweden

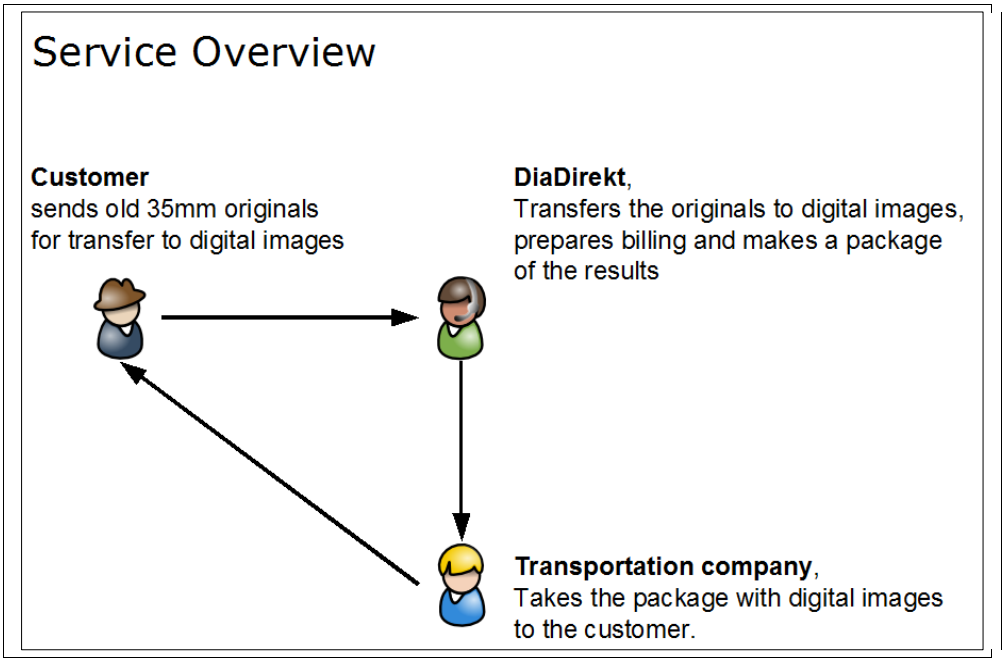
5. Certification Body:

   Unabhängiges Landeszentrum fuer Datenschutz Schleswig-Holstein

   Address: Holstenstr. 98, DE-241 03 Kiel, Germany

6. Specification of Target of Evaluation (ToE):

The target of this evaluation is the IT-service offered under the name DiaDirekt.



The evaluation covered the following main processes:

1. From order to payment (scanning, burning and sending)
2. Administration of customer record for newsletters
3. Sort out digital images and destruct originals images
4. Bookkeeping
5. Business planning

The target of this evaluation does not include:

- The web hosting service and email service
- Transmission via the Internet
- Transportation using a transportation company

In the following sections, the main considerations are presented to the public.

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

Main operation is the collection, storage, use and transmission of customer data to carry out the service to convert original images to digital files burned on DVD or CD.

Furthermore, a minimalistic customer database (spreadsheet and e-mail list) is used for the purpose of sending marketing letters to customers. Personal information adhering to the customers is also processed for the purpose of bookkeeping and business planning.

8. Transnational issues:

The service is offered globally via www.diadirekt.se (in Swedish) and www.diadirekt.com (in English).

The service is not performed over the Internet *per se*, but is a mail order service which recruits customers via the Internet. It requires original images to be sent to the company before converting them to digital images.

As all data handling is performed in a European member state, the European Directive 95/46/EC is applicable.

9. Tools used in the processes:

Orders are received as physical packages, where an order form with instructions has been sent by the customer together with the original images to be transferred. The order forms are stored in paper binders while the orders are being completed.

In the production facilities a network consisting of standard components, router and switch, connect PCs and professional scanning hardware with printer and data storage on NAS-HDD. All hardware is manufactured by well-known global brands. The software used in the production is either licensed from commercial third parties or based on open source.

Administration of customer data is managed in separate standard PC:s connected to the Internet and mail server via modem. Both the PC and modem are manufactured by well-known global brands. The software used in the administration is either licensed from commercial third parties or based on open source.

10. Version of EuroPriSe Criteria Catalogue for Experts used for the evaluation:

Version 0.2

11. Evaluation results:

The evaluation has included an in depth examination based on the European Law and regulations. An overview of the most important aspects are presented.

Work flow

No data is collected unless the customer providing it to the company.

The input data receives in the form of a package, typically containing:

- an order form that the customers fills in. Through the form, the customer is offered the (opt-in) option of providing an e-mail address to receive confirmation of the order and an expected delivery date. The customer is also offered, as opt-in, to join a newsletter.
- Original images to be transferred to disc.

When the package has been received, a sequential order number is created. If the customer has provided an e-mail address a confirmation e-mail with order number and expected delivery date is sent. The order number is used to to substitute name and address during transfer of images according to the customer instructions.

When the transfer is completed, the results and the order number are matched with the original order form to quality assure the results. When the order is completed, the results are sent back to the customer. After an order has been completely processed

any digital image data is securely erased from harddisks.

Customers can choose whether to have their original images sent back or to have also them securely destroyed by the company.

- If the customer wants the originals returned, they are sent back insured against loss or damages.
- If the customer wants the originals destroyed, they are securely destroyed in a heavy-duty electric shredder at the earliest 1 week after the service is completed, and no later than 3 months after the service is completed.

In order to fulfill the Swedish requirements of bookkeeping the company stores book keeping records for 10 years.

To perform business planning the company uses parts of the personal data (name, order number, order information) to produce anonymous statistical data. The personal data is erased annually. The anonymous business planning data is copied to a separate file without links back to individuals. This is stored for 10 years to be able to back track historical development on seasonal variations etc.

If the customer has opted to join the newsletter the email address and name is stored in the address book of the company's e-mail system. The customer is informed of having been listed for the newsletter service, with a clear instruction on how to unsubscribe.

Legitimacy of processing data

The transfer of images is always performed on behalf of the customers. This is underpinned by the general conditions for the service published on the DiaDirekt web site. However, as “private” customers (processing pictures in the course of a purely personal or household activity) are not controllers in the sense of the Directive, the provisions on processing on behalf of the customer are not always (directly) applicable.

It was not the intention of the EU data protection legislator to prohibit the offering of a professional scanning service. Thus, as the company complies with the regulations and formalities of the directive, irrespective of the customer being a commercial customer or not, it is appropriate to apply the provisions on processing on behalf of the customer.

Customers as well as persons depicted on images can exercise their rights of access, correction, erasure and blocking against Tsevnic KB and are informed about this on the DiaDirekt website.

Secure processing

The company has comprehensive security routines documented an implemented.

Order number is used instead of identifiable customer data in the production network and specific security software is activated to protect the data when being processed. Administrative PC has specific security software activated to protect the information used for administration. The premises used are secured against fire and theft. The company has insurance coverage.

Images stored at DiaDirekt are securely destroyed within three months after the service has been performed.

Privacy policy and staff compliance

The processing is governed by a quality- and environmental policy. This is supported by a work manual including security aspects, e.g. requirements on non-disclosure and work steps for secure erasure of image data and destruction of original images and the privacy statement which is published on the web site.

The company adheres to the Data Inspection Board's General advice "Security for personal data" (Datainspektionens Allmänna råd "Säkerhet för personuppgifter") and persons handling images are bound by confidentiality agreements.

Sub-contractors

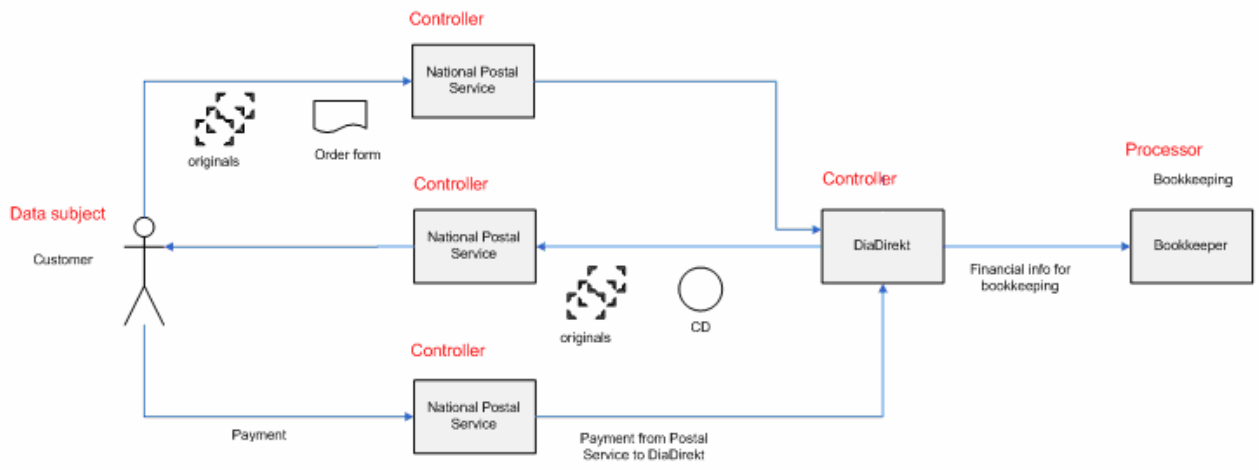
No sub-contractors are used without prior written processing agreements regulating security requirements and legal obligations with regards to handling personal data.

12. Privacy-enhancing functionalities:

The customer has full control over the personal data collected and processed by Diadirekt. There is no personal data collected secretly or surprisingly.

13. Data Flow:

14.



15. Issues demanding special user attention:

The image contains in some cases information constituting sensitive personal data.

16. Compensation of weaknesses:

N/A

17. Decision table on relevant requirements:

Please fill in a decision on all high level requirements listed below and provide some remarks on the main reasons for each decision. The decisions shall cover the processing of primary as well as of secondary data. Making your decisions, you should consider all applicable low level requirements (e.g., high level requirement = 1.2.2 Transparency; low level requirements = 1.2.2.1 and 1.2.2.2).

EuroPriSe Requirement	Decision	Remarks

Data Avoidance and Minimisation	Excellent	All mandatory handling of personal data is to fulfil the service obligations to the customers and to perform business planning. Only order numbers are used to identify customers under production. The customer has the choice to communicate through e-mail or traditional mail.
Transparency	Adequate	The service is accurately described for users and data subjects at www.diadirekt.se and www.diadirekt.com in the Swedish and English language. For experts and other auditors the processes within the service are well described in flowcharts and process handbook.
Technical-Organisational Measures	Adequate	Due to the limited size of the company the implemented administrative and technical measures must be considered mature and comprehensive.
Data Subjects' Rights	Adequate	The customer has full control over the personal data recorded or handed over to Tsevnic KB. The company is also able to provide the data subjects with all relevant information adhering to them in a timely manner. Customers as well as persons depicted on images can exercise their rights of access, correction, erasure and blocking against Tsevnic KB and are informed about this on the DiaDirekt website.

Experts' Statement

I 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.

Place, date Name of Legal and Technical Expert Signature

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 service in a way compliant with European regulations on privacy and data security.

Place, date	Name of Certification Body
Signature	