Short Public Report

on the IT product and IT-based service

ProCampaign 2.0

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

IT product: ProCampaign, version 2.0

IT-based service: ProCampaign, functional status: February 2012

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

Company Name: Consultix GmbH

Company Address: Wachtstrasse 17-24, 28195 Bremen, Germany

Web: https://www.consultix.net

Contact Person: Andres Dickehut, CEO Consultix GmbH

3. Time frame of evaluation:

2009/11/01 – 2012/02/24

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

Name of the Legal Expert: Dr. Irene Karper

Address of the Legal Expert: datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Germany

ikarper@datenschutz-cert.de

Name of the Technical Expert: Ralf von Rahden

Address of the Technical Expert: datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen, Germany

rrahden@datenschutz-cert.de

5. Certification Body:

Name: Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig Holstein

(Independent Centre for Privacy Protection (ULD) Schleswig-Holstein

Address: Holstenstr. 98

24103 Kiel, Germany

eMail: europrise@datenschutzzentrum.de

6. Specification of Target of Evaluation (ToE):

ProCampaign, version 2.0, is a multi-functional web based application to support the Customer Relationship Management (CRM) used by public authorities (e.g. in the field of tourism or city marketing) or companies, especially internationally oriented business.

Vendor is the Consultix GmbH (limited) with its headquarter in Bremen, Germany, which continuously develops the application and which hosts the systems (on behalf of the contracting party) in an self-owned data center. Therefore, the evaluated target is an IT product as well as an IT-based service, however the application is consistently called "ProCampaign".

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

The focus of ProCampaign is the collection and processing of personal data to support the CRM. Users are companies or bodies using ProCampaign for their own purposes. The Consultix GmbH also operates as the data processor of the IT-based service "ProCampaign".

7.1 Purpose and area of application

The user collects and processes data of consumers or end users by means of ProCampaign. It typically relates to natural persons. To support the CRM, personal data of consumers are fed into the database of ProCampaign and can be evaluated or conditioned for market analysis, consumer retention measures or to optimize marketing campaigns. ProCampaign is designed as a data warehouse and allows the user to manage data that he receives through various marketing campaigns. The user can either transfer existing own customer data

in ProCampaign, or in the context of a participation of consumers for an online-marketing campaign (e.g. via an electronic newsletter, online sweepstakes or online registrations for closed user groups) the user generates new data, which are directly transferred by data fields on the website (so called transaction).

The definition of the data fields and the processing by ProCampaign lies within the legal responsibility of the user. ProCampaign supports compliance with the relevant data protection provisions by providing the user with an informative leaflet on data protection which supports the user in the legally compliant establishment and use of ProCampaign. Also the origin of data generated and stored in the system ProCampaign can be traced at any time according to the basis of the respective transaction.

The focus of ProCampaign however is mainly the so-called permission marketing, i.e., it supports the obtaining and (traceable and provable) management of consent statements in the respective data collection and data processing. Need for and requirements of consent of the consumer in data collection and data usage vary depending on the means of communication of direct advertising and the respective legal provision.

In the European Union, provisions can be found in Directive 95/46/EC and its various forms in national law. The legal basis for data proceeding is stated in article 7 of the Directive 95/46/EC. As stated in article 7 lit. a) of the Directive, the basis for data proceeding can be a data subject´s consent, as defined in article 2 lit. h) of the Directive. It states, that the data subject's consent is any expression of will, which is carried out without coercion, specific and informed and with which the person concerned accepted processing of personal data that concern him.

In accordance with article 14 lit. b) of the Directive 95/46/EC, the data subject has the right to object to the processing of personal data for the purposes of direct marketing (Opt-Out). Characteristics of this regulation can be found in German law in articles 4, 4a and 28 of the Federal Data Protection Act (FDPA).

However, for the processing of personal data by email, telefax or automatic call systems, Article 13 of the Directive 2002/58/EC states an Opt-In as a restrictive

regulation, which found entrance in the German law in article 7 of the Act Against Unfair Practices (AAUP).

According to German law, direct marketing by email, phone or short message service (sms) always requires (in accordance with article 7 of the AAUP) an explicit consent (opt-in), while advertising via mail according to the so called "list privilege" of article 28 FDPA therefore follows the opt-out principle for the possibility of opposition.

For advertising or statistical analysis using electronic communication, special specifications are also pursuant to Directive 2002/58/EC. For example, the analysis of consumers' click behavior on web portals or through links to websites in newsletters as well as the forwarding of newsletters themselves are generally subject to consent (cf. article 13 of Directive 2002/58/EC and section 7 of the German AAUP). The stipulations of article 5 (3) of Directive 2002/58/EC must also be observed, if cookies are used, respectively if information is stored or retrieved on the end user's device.

These provisions have been inter alia substantiated by the declaration of the Article 29 Data Protection working Party (cf. Working Paper No. 148, p. 14 and Working Paper Nr. 159, p. 5, n. 7), inter alia, and by the EuroPriSe certification bodies in a position paper („Position paper on the impact oft he new „cookie law" on certifiability of behavioral advertising systems according to EuroPriSe", July 2010) as well.

By means of ProCampaign, an opt-in or opt-out can be stored in the system depending on the communication channel and transaction and it can be taken into account for future marketing campaigns. In the context of the registration to receive an email newsletter the so-called "double-opt-in" procedure is applied, i.e. the consumer signs up for the email newsletter and will receive an email to the specified address with a request to confirm the order by clicking on a link; he receives the newsletter only after confirmation. The double-opt-in process assures in greatest extent that the recipient has actually consented to receiving advertising emails so that this marketing does not represent undue harassment.

On the basis of filed transactions it is also traceable at any time, whether relevant changes to the marketing campaign were made, such as the change of the privacy information for the consumer.

Here too, the user remains legally responsible for the data collection and use of information for advertising purposes. He is made aware on the requirements in the course of the use of ProCampaign in form of the aforementioned leaflet with explanatory remarks about privacy. This information sheet is available both in German and in English language.

It is to highlight that a data protection concept based on German law was developed for ProCampaign. In this concept, the admissibility of data processing under different legal aspects (e.g. FDPA, Act Against Unfair Practices, Telemedia Act) relating to practical use by the user was assessed and evaluated.

The data base of ProCampaign can also be separated for different user clients so that for each client a separate data collection and data usage can be established, e.g. in international companies. ProCampaign offers an exemplary differentiated roles and authorization concept for the access of the user to its data. This allows the user to grant always only the access needed for the respective roles.

7.2 Audited range of functions in the standard version

ProCampaign in the audited version includes the following functions:

- Obtaining and management of the consent of the consumer

  Creating and depositing declarations of consent (opt-in), as well as of contradictions (opt-out) for identifiable means of communication.

- Deduplication of records

  A built-in duplicate detection based on specific criteria, prevents that several database profiles are created in ProCampaign

- Assignment of registration numbers

Assigning unique registration number facilitates the identification of persons and actions. These registration numbers are generated in the database and checked afterwards.

- Exclusion of certain users

With this function, consumer data can be excluded from actions, e.g. in case of a dissent in data proceeding for marketing purposes.

- Cleaning up data

Data not achievable and inactive profiles are deleted after a pre-defined procedure. Secondary data are also automatically deleted after certain periods of time. The duration of logging secondary data depends on the content and the purpose of the log file.

- Evaluation and analysis of resource

With this function analysis can be realised.

- Data selection

This function allows the user to address offline or online mailings targeted to specific target groups. These target groups are selected from the database, based on specific criteria.

- ProComplaint

This is a form for complaints management, which the user runs in his own call center.

The range of the standard version also includes the IT-based service of Consultix GmbH on behalf of the user, in particular hosting ProCampaign.

7.3 Functions outside the approved standard

ProCampaign can be extended on request with optional features that are outside of the evaluation. Optional features of ProCampaign that do not belong to the standard scope are:

- Postal address- and name-check and correction;

- Postal address check after moving;

- determination of the "most valuable consumer";

- investigation and clarification of violations of the relevant terms and conditions of the customer in the context of illicit multiple registrations or by voucher / coupon fraud;

Data collection on users and consumers, provision of services other than ProCampaign by Consultix GmbH, the environment for the user, consumer, and fulfilment partner, as well as the accounting processes between Consultix GmbH and the users are not part of the scope of ProCampaign.

Also, the user's media interfaced via ProCampaign are not subject of the basic product and therefore not target of evaluation (in particular websites, call center of the user).

8. Transnational issues:

Since ProCampaign is a web based application it can be used worldwide. The majority of companies deploying ProCampaign at present are domiciled in Germany. Some, though, deploy ProCampaign at their branches within the European Union, the EEA or worldwide.

ProCampaign Systems and Server are located in the data center of Consultix GmbH within the Federal Republic of Germany.

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

Concerning ProCampaign, all IT systems are controlled by monitoring tools which inform the administration about irregularities.

All actions on IT systems are logged revision-proof. The network monitoring exists on different levels:

- "WhatsUp Gold" allows for controlling of hardware (CPU-load, hard disk capacity, capacity of random access memory) and server services.

Therefore, two additional monitors have been installed in the administration rooms;

- "Traffic Monitoring" is carried out for controlling the bandwidth on routes (Cacti);

- "Tipping Point" controls the incoming network packages for purposes of network attack identification;

- "Netflow" is carried out for billing purposes, based on socket layer access recorded on the firewall;

- Additionally "Syslog" has been installed on all router and Unix systems;

By means of these packages of monitoring tools, security of all data is assured on a very high level.

10. Edition of EuroPriSe Criteria used for the evaluation:

The experts used EuroPriSe Criteria Catalogue, version May 2011 and EuroPriSe Glossary, Version 1.0.

Note: Alongside the evaluation according to EuroPriSe, ProCampaign was also evaluated according to the standard of the privacy seal due to the federal state order of Schleswig-Holstein on a privacy audit (Schleswig-Holsteinische Landesverordnung über ein Datenschutzaudit, DSAVO).

11. Evaluation results:

The following outstanding results could be found within the framework of the audit:

11.1 Implementation of legal requirements

The technical solutions used by ProCampaign innovatively enable the implementation of the legislative requirements.

The collection of data by means of ProCampaign is determined only by the respective user. The data collected in ProCampaign is used in particular for directly addressing the consumer for advertising purposes and the assessment

of statistical evaluation. ProCampaign is thus designed to promote the permission marketing, i.e. the consumer data is basically saved and as a result of the submission of a declaration of consent in ProCampaign processed.

Therefore, ProCampaign provides the compliance with the provisions of article 13 of the Directive 2002/58/EC, article 7 AAUP also as article 14 lit. b) of the Directive 95/46/EC respectively article 28, section 4 FDPA.

Also, the implementation of legal requirements (for example, FDPA, Act Against Unfair Practices, Telemedia Act) is regularly being assessed and evaluated, in particular due to the data protection concept developed for ProCampaign with regard to the user's practical use.

By operating ProCampaign, no cookies are used; therefore the provisions of the European „Cookie Directive" do not directly apply. The described data sheet indicates however the user the information requirements for the use of cookies, as well as on the requirements of the EU directives. The given information is orientated on the provisions of EuroPriSe certification bodies by the „Position paper on the impact of the new „cookie law" on certifiability of behavioral advertising systems according to EuroPriSe".

Therefore, the user is made aware of legal requirements for the data collection and use of data by the described information sheet on the fulfilment of the requirements in an exemplary way.

11.2   Data avoidance

In addition, ProCampaign provides functions to avoid or minimise processing of personal information, such as:

- the use of pseudonyms in consumer registration,

- anonymous analysis,

- a detailed concept for deletion, blocking or cleaning of consumer data and

- a differentiated authorization concept; access to personal data within the system of ProCampaign can thus be limited to need-to-know-basis.

The user is explicitly pointed towards the principles of data avoidance and data minimization by the information sheet and is asked to comply with them for the individual establishment and use of the system.

11.3 Data security

The servers are operated in a data center with strong admittance and access controls. All data transfers within the use of ProCampaign are secured via SSL (RSA-1024). Also, the data is backed up appropriately following a backup policy.

The statutory retention periods for certain data relevant to taxation and commerce law regulations can be guaranteed by the backup policy. The Consultix GmbH is committed to review this concept within the validity of the certification with regard to the principles of necessity, data reduction and data minimization and adjust if necessary.

11.4 Implementation of consumers' rights

ProComplaint enables consumers to exercise their right of access via the integrated call center. In addition, consumers may also ask for correction and deletion. Also, adherence of consumers' rights is promoted by pointing out the implementation in the leaflet to the user.

12. Data flow:

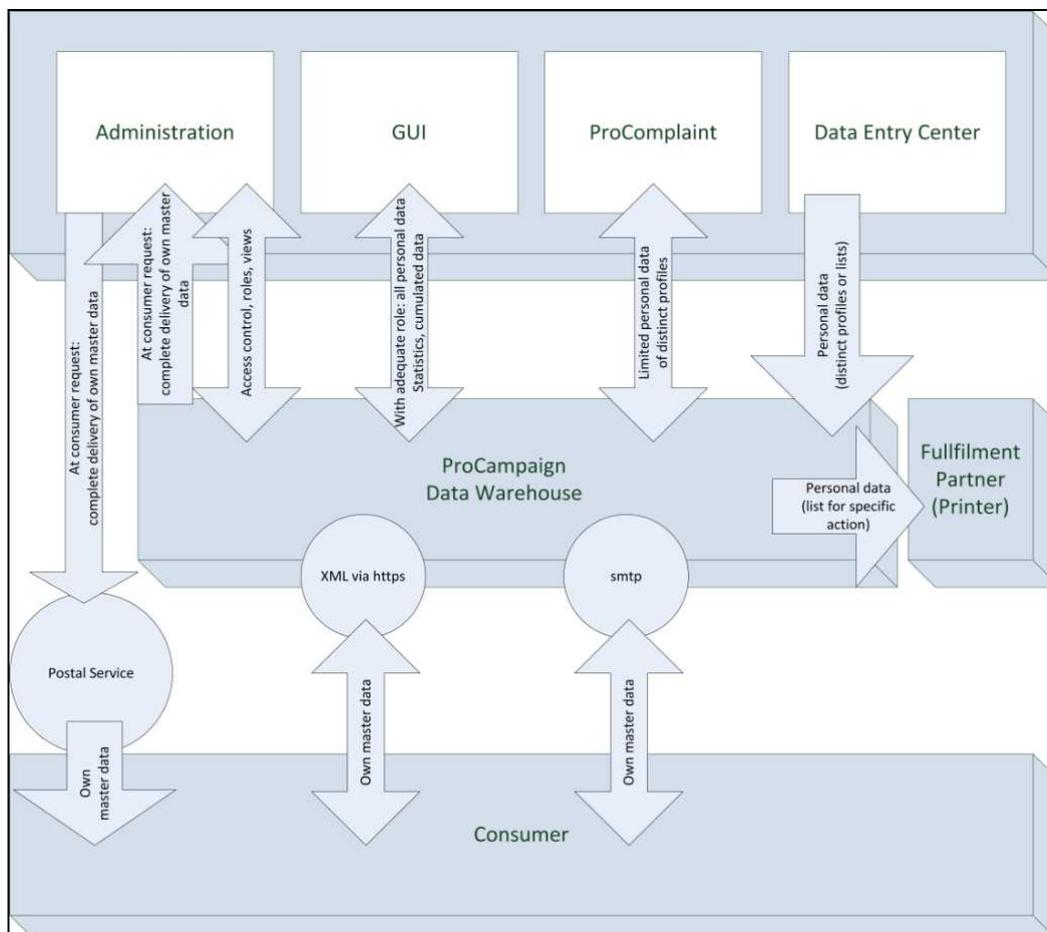The following graphic describes the data flow of ProCampaign:

Illustration 1: data flow

13. Privacy enhancing functionalities:

ProCampaign contains the following privacy enhancing functionalities:

- Data confidentiality is assured by the authorization concept which allows differentiated access rights;

- The description of the product and information of data processing are transparent and reasonably completed by individual training;

- ProCampaign has an blacklist to store anonymous dissents in data processing by filing hash codes;

- Organizational and technical measures for granting data security and privacy are above legal standard;

- The data processor is sensitizing the user to privacy compliance in an exemplary way;

- A high availability of data is made possible by a multilevel backup concept and redundancy of infrastructure.

14. Issues demanding special user attention:

The evaluation did not rate any of the issues as "additional safeguards needed". Nevertheless the privacy compliant use of ProCampaign lies within the responsibility of the user. He must adopt the given information by the developer about privacy standards and privacy enhancing configuration of ProCampaign.

15. Compensation of weaknesses:

Since ProCampaign does not pass any requirement with the grade "barely passing", there is no need to compensate a shortcoming.

16. Decision table on relevant requirements:

EuroPriSe Requirement	Decision	Remarks
Data Avoidance and Minimisation	adequate	ProCampaign allows collecting different data of consumers; data avoidance and data minimisation lies in the responsibility of the user; nevertheless ProCampaign allows anonymisation of transactions concerning consumer data. It also allows the user to delete consumer data and secondary data such as log files within a short, sufficient time.
Transparency	excellent	Documentation and fact sheets on behalf of compliance and privacy are informative, up-to date and understandable; the processor also provides information for risk assessment, security policies and a privacy concept.
Technical-Organisational Measures	excellent	Organizational and technical measures on data security and privacy are above legal standard. The self-owned data center of the processor is located in Bremen, Germany and complies with all standards in regard to physical access control, recovery mechanism, network and transport security on a high level. The IT infrastructure is well-documented; a security policy is in place. Employees are well trained on privacy and data security matters.
Data Subjects' Rights	adequate	ProComplaint provides a feature that allows users to react on consumer questions or dissents in data proceeding; data Subjects can easily declare an opt-in or an opt-out dependent on their choice; also the data processor is sensitizing the user to implement data subject´s rights.

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.

Bremen, 2012-03-19   Dr. Irene Karper LLM.Eur.

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2012-03-19   Ralf von Rahden

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 protection.

Kiel,	Independent Centre for Privacy Protection (ULD) Schleswig-Holstein	
Place, Date	Name of Certification Body	Signature