Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für „ProCampaign 2.0“

im Auftrag der Consultix GmbH

datenschutz cert GmbH

13.03.2012

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	13.03.2012	alle	Finalisierung	Dr. Irene Karper, Dipl. Math. Ralf von Rahden

1. Über die Auditierung von ProCampaign

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung des Verfahrens „ProCampaign“ in der Version 2.0 dokumentiert, mit welcher die datenschutz cert GmbH seitens der Consultix GmbH beauftragt wurde.

ProCampaign ist eine multifunktionale, webbasierte Anwendung zur Unterstützung des Customer Relationship Management (CRM), welches sowohl bei öffentlichen Stellen (z.B. im Bereich Tourismus oder Stadtmarketing) als auch in der Privatwirtschaft, insbesondere bei international agierenden Unternehmen, einsetzbar ist.

Hersteller ist die Consultix GmbH aus Bremen, welche die Anwendung fortlaufend entwickelt und für Vertragspartner („Anwender“) im eigenen Rechenzentrum hostet. Insofern handelt es sich bei dem auditierten Gegenstand sowohl um ein IT-Produkt (ProCampaign in der Version 2.0) als auch um einen IT-basierenden Service. Die Anwendung insgesamt wird nachfolgend als ProCampaign bezeichnet.

Die Prüfung wurde parallel anhand des Standards des Datenschutz-Gütesiegels gemäß der Schleswig-Holsteinischen Landesverordnung über ein Datenschutzaudit (DSAVO) [1] sowie gemäß dem Standard „EuroPriSe“ durchgeführt. Grundlage für die Erstellung dieses Kurzgutachtens gemäß DSAVO ist die Version 1.2 des Anforderungskatalogs für ein Datenschutz-Gütesiegel des ULD. Die Zusammenfassung der Ergebnisse der EuroPriSe-Evaluation bleiben einem gesonderten Bericht vorbehalten, der an anderer Stelle veröffentlicht ist[2].

Im Ergebnis stellen die Auditoren fest, dass ProCampaign in der Version 2.0 unter Beachtung der dem Anwender zur Verfügung gestellten Datenschutzhinweise konform zu den gesetzlichen Anforderungen an den Datenschutz und die Datensicherheit eingesetzt werden kann und dass ProCampaign in der Version 2.0 in der Standardausführung unter Beachtung der Datenschutz-Hinweise in besonderem Maße den Datenschutz beim Anwender fördert.

2. Antragstellerin

Antragstellerin der Auditierung und Zertifizierung gemäß DSAVO ist die

Consultix GmbH
Wachstraße 17
28195 Bremen

als Hersteller des IT-Produkts ProCampaign und als IT-Service-Dienstleister. Ansprechpartner ist Herr Andres Dickehut, Geschäftsführer der Consultix GmbH.

---

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) v. 18.11.2009, *GVOBl.* Schl.-H. *2008, S. 562ff. / GVOBl.* Schl.-H. *2009, S. 742ff.*
[2] Online abrufbar unter https://www.european-privacy-seal.eu/ (Stand: 02/2012).

3. Sachverständige Prüfstelle

Sachverständige Prüfstelle gemäß DSAVO ist die

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0421-696632-50
E-Mail: office@datenschutz-cert.de
Web: www.datenschutz-cert.de

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Dr. Irene Karper (Recht). Ansprechpartner für diese Auditierung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik). Beide Ansprechpartner sind zugleich beim ULD als EuroPriSe-Experts zugelassen.

4. Zeitraum der Prüfung

Die Auditierung von ProCampaign erstreckte sich auf den Zeitraum von 01.11.2009 bis 24.02.2012 und beinhaltete neben der konzeptionellen Analyse der von der Consultix GmbH zur Verfügung gestellten Dokumente auch die Durchführung von Plausibilitätstests der Anwendung und der Besichtigung des IT-Services vor Ort.

5. Kurzbezeichnung der Anwendung

Auditiert wurde das IT-Produkt ProCampaign in der Version 2.0 sowie der IT-basierende Service anhand des Funktionsstands vom Februar 2012.

6. Beschreibung der Anwendung

Im Fokus von ProCampaign steht die Erfassung und Verarbeitung von personenbezogenen Daten zur Unterstützung des CRM. Anwender sind Unternehmen oder Stellen, die ProCampaign für eigene Zwecke nutzen. Die Consultix GmbH wird im Rahmen des IT-basierenden Services als Auftragsdatenverarbeiter tätig.

6.1 Zweck und Einsatzbereich

Der Anwender erfasst und verarbeitet mittels ProCampaign Daten von Konsumenten oder Endverbrauchern. In der Regel handelt es sich hierbei um natürliche Personen. Zur Unterstützung des CRM werden personenbezogene Daten des Konsumenten in die Datenbank von ProCampaign eingespeist und können für Marktanalysen, Kundenbindungsmaßnahmen oder zur Optimierung von Marketingkampagnen ausgewertet oder aufbereitet werden. ProCampaign ist als „Data Warehouse“ konzipiert und ermöglicht dem Anwender Daten zu verwalten, die er über verschiedene Marketingaktionen erhält. Der Anwender kann entweder vorhandene Konsumentendaten in ProCampaign überspielen oder im Rahmen der Teilnahme eines Konsumenten an einer Online-Marketingaktion (z.B. über einen elektronischen Newsletter, über Online-Gewinnspiele oder Online-Registrierungen für geschlossene Benutzergruppen) Daten generieren, die direkt über die Datenfelder auf einer Webseite des Anwenders in die Datenbank von ProCampaign übertragen werden (sogenannte Transaktion).

Die Definition der Datenfelder und die Verarbeitung mittels ProCampaign liegen in der rechtlichen Verantwortung des Anwenders. ProCampaign unterstützt die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben, indem dem Anwender ein informatives Merkblatt zum Datenschutz anhand gegeben wird, welches den Anwender bei der rechtskonformen Einrichtung und Nutzung von ProCampaign unterstützt. Zudem kann die Herkunft der generierten und gespeicherten Daten im System ProCampaign jederzeit anhand der jeweiligen Transaktion entsprechend nachvollzogen werden.

Im Fokus von ProCampaign steht vor allem aber das sogenannte Permission-Marketing, d.h., es unterstützt die Einholung sowie nachvollziehbare und beweisbare Verwaltung von Einwilligungserklärungen in die jeweilige Datenerfassung und Datenverarbeitung. Notwendigkeit und Anforderungen einer Einwilligungserklärung des Konsumenten in Datenerfassung und Datennutzung sind – je nach Kommunikationsmittel - unterschiedlich. Etwa erfordert die Direktwerbung mittels E-Mail, Telefon oder Short Message Service (sms) gemäß § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) und § 28 BDSG i.V.m. §§ 4, 4a Bundesdatenschutzgesetz (BDSG) nach deutschem Recht immer eine ausdrückliche Einwilligung (Opt-In), während Werbung per Postsendung nach dem Listenprivileg des § 28 BDSG in der Regel nur einen Hinweis auf und die Möglichkeit des Widerspruchs (Opt-Out) fordert.

Mittels ProCampaign können Opt-In oder Opt-Out des Konsumenten im System je nach Kommunikationskanal und Transaktion hinterlegt und für künftige Marketingaktionen berücksichtigt werden. Im Rahmen der Anmeldung für den Empfang eines E-Mail-Newsletters wird dabei das sogenannte Double-Opt-In-Verfahren angewendet, d.h. der Konsument registriert sich für den E-Mail-Newsletter, erhält eine E-Mail an die angegebenen Adresse mit der Bitte, die Bestellung per Klick auf einen Link zu bestätigen und erhält erst nach Bestätigung den Newsletter. Mit dem Double-Opt-In-Verfahren kann so in größtmöglichem Umfang sichergestellt werden, dass der Empfänger auch tatsächlich in die Verwendung seiner Daten eingewilligt hat und z.B. der Empfang von Werbe-E-Mails für Ihn keine unzumutbare Belästigung darstellt.

Anhand der hinterlegten Transaktionen ist zudem jederzeit nachvollziehbar, ob an der Marketingaktion relevante Änderungen durchgeführt wurden, wie z.B. die Änderung der Datenschutz-Informationen für den Konsumenten.

Rechtlich verantwortlich für die Datenerfassung und Datennutzung zu Werbezwecken bleibt auch hier der Anwender. Er wird im Zuge des Einsatzes von ProCampaign in Form des bereits erwähnten Merkblatts mit Hinweisen zum Datenschutz auf die Anforderungen sensibilisiert. Das Merkblatt steht sowohl in deutscher als auch in englischer Sprache zur Verfügung.

Hervorzuheben ist, dass für ProCampaign ein Datenschutzkonzept nach deutschem Recht entwickelt wurde. Darin wird die Zulässigkeit der Datenverarbeitung unter verschiedenen rechtlichen Aspekten (z.B. BDSG, UWG, Telemediengesetz) im Hinblick auf den praktischen Einsatz beim Anwender geprüft und bewertet.

ProCampaign lässt sich ferner nach Anwender-Mandanten trennen, so dass z.B. auch in internationalen Konzernen eine jeweils getrennte Datenerfassung und Datennutzung eingerichtet werden kann. Für den Zugriff des Anwenders auf seine Daten bietet ProCampaign ein vorbildlich differenziertes Rollen- und Berechtigungskonzept. Auf diese Weise ist es dem Anwender möglich, verschiedenen Rollen nur den Zugriff zu gewähren, der jeweils benötigt wird.

6.2 Funktionsumfang der auditierten Standardausführung

Zu ProCampaign in der hier auditierten Version gehören folgende Funktionen:

--- Einrichtung und Verwaltung der Einwilligungserklärung des Konsumenten

Anlegen und Hinterlegen von Einwilligungserklärungen (Opt-In) sowie von Widersprüchen (Opt-Out) für bestimmbare Kommunikationsmittel.

--- Deduplizierung von Datensätzen

Über eine Dublikaterkennung wird nach bestimmbaren Kriterien verhindert, dass Profile mehrfach in der Datenbank angelegt werden.

--- Vergabe von Registrierungsnummern

Durch die Vergabe von eindeutigen Registrierungsnummern wird die Identifikation von Personen und Aktionen erleichtert. Diese Registrierungsnummern werden in der Datenbank generiert und geprüft.

--- Ausschluss bestimmter Konsumenten

Hierüber können Datensätze von Konsumenten von Aktionen ausgenommen werden, etwa bei Vorliegen eines Widerspruchs gegen die Datenverarbeitung zu Werbezwecken.

--- Datenbereinigung

Nicht erreichbare und inaktive Profile werden nach einem festgelegten Verfahren gelöscht.

Sekundärdaten werden ebenfalls automatisch nach bestimmten Zeiträumen gelöscht. Dabei richtet sich die Speicherdauer nach dem Inhalt und dem Zweck der Log Daten.

--- Auswertung und Ressourcenanalyse

Hierüber können Auswertungen realisiert werden.

--- Datenselektion

Diese ermöglicht es dem Anwender, Mailings zielgerichtet an spezifische Zielgruppen zu adressieren. Anhand von bestimmbaren Kriterien werden Zielgruppen aus dem Datenbestand selektiert.

--- ProComplaint

Dies ist eine Eingabemaske für ein Beschwerdemanagement, das der Anwender in einem eigenen Callcenter führen kann.

Zum Standardumfang gehört außerdem der IT-basierende Service der Consultix GmbH im Auftrag des Anwenders, insbesondere das Hosting von ProCampaign.

6.3 Funktionen außerhalb des auditierten Standardumfangs

ProCampaign lässt sich mit optionalen Funktionen erweitern, die außerhalb dieser Auditierung liegen. Nicht zum Standardumfang gehören:

- --- Überprüfung und Korrektur von Postadressen, Namen,
- --- Überprüfung von Adressänderungen durch Umzug,
- --- Ermittlung des „Most Valuable Consumers“,
- --- Ermittlung und Aufklärung von Verstößen gegen die jeweiligen Teilnahmebedingungen des Anwenders im Rahmen von unerlaubten Mehrfachregistrierungen oder durch Gutschein-/Coupon-Betrug.

Die Datenerfassung beim Anwender und beim Konsumenten sowie alle über den IT-basierenden Service bzgl. ProCampaign hinausgehenden Dienstleistungen der Consultix GmbH, die Einsatzumgebung beim Anwender, beim Konsumenten sowie der Abrechnungsprozess gehören nicht zum Funktionsumfang von ProCampaign.

Ebenfalls nicht zum Standardumfang und damit nicht zum auditierten Gegenstand gehören die über ProCampaign einbindbaren Medien und Kommunikationsmittel (insbesondere Webseiten, Callcenter) des Anwenders.

7. Modellierung des Datenflusses

Mittels ProCampaign werden sowohl Primärdaten als auch Sekundärdaten verarbeitet.

7.1 Primärdaten

- --- In ProCampaign werden personenbezogene oder –beziehbare Daten des Konsumenten erfasst, die dieser anhand der vom Anwender definierten Datenfelder erfasst und die an die Datenbank von ProCampaign übermittelt werden. In der Standarddefinition sind dies Name, Postadresse und Geburtsdatum. Der Anwender kann weitere Attribute definieren.
- --- Weitere personenbezogene Daten können als Kommentar per Freitextfeld über ProComplaint eingegeben werden. In der Regel bezieht sich ein Kommentar auf einen Geschäftsvorgang, nicht auf eine Person.
- --- Ferner werden die Registrierungsnummer eines Konsumenten sowie Transaktionsdaten und das dazugehörige Attribut (z.B. Gewinnspielteilnehmer, Produkttester etc.) erfasst. Transaktionsdaten sind ohne Attribute nicht personenbeziehbar.
- --- Beim elektronischen Newsletter wird das Nutzerverhalten anhand der angeklickten und geöffneten Positionen erfasst.
- --- Schließlich ist die IP-Adresse des anfragenden Rechners des Konsumenten ein Primärdatum.

7.2 Sekundärdaten

Sekundärdaten sind administrative Daten, also Log Daten auf Anwendungsebene (Webserver Logfiles sowie API Logfiles), welche eine IP-Adresse als einzige personenbeziehbare Information enthalten.

7.3 Datenfluss

Der Datenfluss mittels ProCampaign lässt sich wie folgt darstellen:

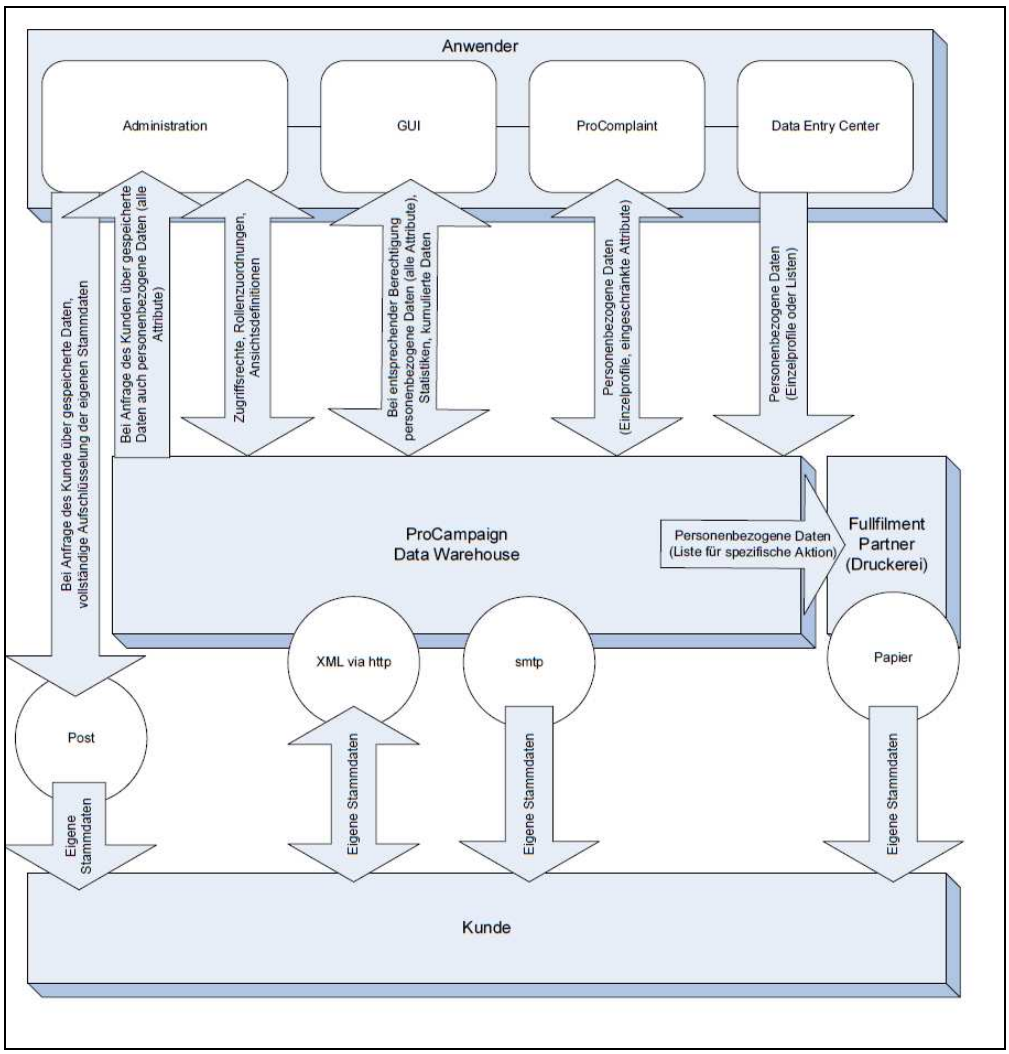

Abbildung 1: Datenfluss von ProCampaign

8. Eingesetzte Tools

Sämtliche IT-Systeme im Hinblick auf ProCampaign werden durch Monitoring-Tools überwacht, die den Administrator bei Unregelmäßigkeiten informieren. Alle Tätigkeiten auf den IT-Systemen werden nachvollziehbar protokolliert. Das Netzwerk-Monitoring erfolgt auf verschiedenen Ebenen:

--- WhatsUp Gold dient zur Überwachung der Hardware (CPU-Last, Festplattenkapazität, Arbeitsspeicherauslastung) und Serverdienste. Hierzu sind zwei zusätzliche Bildschirme in den Räumen der Administratoren installiert;

--- Traffic Monitoring erfolgt zur Überwachung der Bandbreite auf den Routern (Cacti);

--- Tipping Point überwacht die eingehenden Netzwerkpakete zwecks Erkennung von Netzwerkattacken;

--- Netflow wird zu Abrechnungszwecken eingesetzt und basiert auf Socketverbindungen, die in der Firewall registriert werden;

--- Zusätzlich ist auf allen Routern und Unixsystemen Syslog installiert;

Mit Hilfe dieses Pakets von Monitoring-Tools wird die Sicherheit sämtlicher Daten in sehr hohem Maße gewährleistet.

9. Herausragende Prüfergebnisse

Im Rahmen der Auditierung konnten folgende herausragende Prüfergebnisse festgestellt werden:

9.1 Umsetzung von rechtlichen Anforderungen

Die mittels ProCampaign verwendeten technischen Lösungen ermöglichen innovativ die Umsetzung der gesetzlichen Vorgaben.

Die Datenerfassung mittels ProCampaign wird vom jeweiligen Anwender bestimmt. Dabei dienen die in ProCampaign erfassten Daten insbesondere der werblichen Direktansprache des Konsumenten oder der statistischen Auswertung. ProCampaign ist dabei so konzipiert, dass es das Permission-Marketing fördert, d.h., die Konsumentendaten werden grundsätzlich erst infolge der Abgabe einer Einwilligungserklärung in ProCampaign gespeichert und nutzbar gemacht.

Die Umsetzung rechtlicher Anforderungen (z.B. BDSG, UWG, TMG) wird insbesondere durch das für ProCampaign entwickelte Datenschutzkonzept im Hinblick auf den praktischen Einsatz beim Anwender regelmäßig geprüft und bewertet.

Der Anwender wird über das beschriebene Merkblatt auf die Einhaltung der rechtlichen Anforderungen bei der Datenerfassung und Datennutzung sensibilisiert.

9.2 Datensparsamkeit

Darüber hinaus bietet ProCampaign Funktionen zur Vermeidung von personenbezogenen Daten, wie etwa:

--- die Nutzung von Pseudonymen bei Konsumentenanmeldung;

--- anonymisierte Auswertungen;

--- ein detailliertes Konzept zur Löschung, Sperrung oder Bereinigung von Konsumentendaten;

--- ein sehr differenzierbares Berechtigungskonzept; Der Zugriff auf personenbezogene Daten innerhalb des Systems von ProCampaign kann damit auf das jeweils notwendige Maß begrenzt werden.

Der Anwender wird durch das Merkblatt auf die Einhaltung der Grundsätze der Datenvermeidung und Datensparsamkeit explizit hingewiesen und aufgefordert, diese bei der individuellen Einrichtung und Nutzung des Systems zu beachten.

9.3 Datensicherheit

Die Server werden in einem Rechenzentrum mit starken Zugangs- und Zugriffskontrollen betrieben. Sämtliche Datentransfers mit ProCampaign werden per SSL (RSA-1024) gesichert. Zudem werden die Daten über ein Backupkonzept angemessen gesichert.

Die gesetzlichen Aufbewahrungsfristen bestimmter steuerrechtlich- und handelsrechtlich relevanter Daten können über das Backupkonzept gewährleistet werden. Die Consultix GmbH hat sich verpflichtet dieses Konzept innerhalb der Gültigkeit der Zertifizierung hinsichtlich der Grundsätze der Erforderlichkeit, Datenvermeidung und Datensparsamkeit zu überprüfen und ggf. anzupassen.

9.4 Umsetzung der Betroffenenrechte

ProComplaint gibt den Konsumenten über das vom Anwender integrierte Callcenter die Möglichkeit, Auskunft über sie gespeicherte Daten zu erfahren und z.B. die Löschung zu beantragen. Zudem wird die Einhaltung der Betroffenenrechte gefördert, indem der Anwender im Merkblatt auf die Umsetzung hingewiesen wird.

10. Gesamtbewertung

Gemäß dem Anforderungskatalog für ein Datenschutz-Gütesiegel in der Version 1.2 konnten die Auditoren folgende Bewertungen treffen:

PRIMÄRDATEN		
Nr.	**Anforderung**	**Bewertung**
A1	Produktbeschreibung	In vollem Umfang sichergestellt
A2	Datensparsamkeit, Pseudonyme	In adäquater Weise sichergestellt
A3	Frühzeitiges Löschen, Anonymisieren	In adäquater Weise sichergestellt
A4	Zulässigkeit der Datenverarbeitung	zulässig
A5	Authentizität	In adäquater Weise sichergestellt
A6	Vertraulichkeit	In vollem Umfang sichergestellt
A7	Integrität	In vollem Umfang sichergestellt
A8	Verfügbarkeit	In vollem Umfang sichergestellt
A9	Revisionsfähigkeit	In vollem Umfang sichergestellt
A10	Betroffenenrechte	In adäquater Weise sichergestellt
SEKUNDÄRDATEN		
Nr.	**Anforderung**	**Bewertung**
B1	Produktbeschreibung	In adäquater Weise beschrieben
B2	Zulässigkeit der Datenverarbeitung	zulässig
B3	Vertraulichkeit	In vollem Umfang sichergestellt
B4	Integrität	In vollem Umfang sichergestellt
B5	Verfügbarkeit	In vollem Umfang sichergestellt

11. Förderung des Datenschutzes

Das Produkt enthält im Sinne der DSAVO folgende, den Datenschutz fördernde Funktionen:

- --- Die Vertraulichkeit der Daten wird durch ein Berechtigungskonzept sichergestellt, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht;
- --- Produktbeschreibung und Informationen zur Datenverarbeitung sind transparent und werden durch individuelle Schulungen sinnvoll ergänzt;
- --- Für die Speicherung von Widersprüchen führt ProCampaign eine anonymisierte Blacklist, die ausschließlich Hashwerte speichert;
- --- Organisatorische und technische Maßnahmen zur Datensicherheit und zum Datenschutz gehen über die gesetzlichen Anforderungen hinaus;
- --- Der Auftragnehmer sensibilisiert den Anwender in vorbildlicher Weise auf die Einhaltung des Datenschutzes;
- --- Es wird eine hohe Verfügbarkeit der Daten durch mehrstufiges Backupkonzept und Redundanz der Infrastruktur ermöglicht.

12. Votum der Auditoren

ProCampaign in der Version 2.0 sowie der dazugehörige IT-basierende Service mit Stand zum Februar 2012 erfüllen die Anforderungen an den Datenschutz und die Datensicherheit gemäß DSAVO in besonderer Weise.

Bremen, 13. März 2012

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH