Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für „ProCampaign 7.0“

im Auftrag der Consultix GmbH

datenschutz cert GmbH
03.02.2017

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	03.02.2017	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 7.0 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 7.0) als auch um einen IT-basierenden Service. Die Anwendung insgesamt wird nachfolgend als ProCampaign bezeichnet.

ProCampaign wurde erstmals in der Version 2.0 gemäß EuroPriSe[1] sowie anhand der damaligen Datenschutzgütesiegelverordnung (DSAVO)[2] zertifiziert. Gegenstand der jetzigen Auditierung ist ProCampaign in der Version 7.0. Funktionsstand des IT-Services ist Januar 2017.

Diese Auditierung wurde dabei sowohl anhand der Datenschutzgütesiegel-verordnung Schleswig-Holsteins (DSGSVO)[3] als auch gemäß dem Standard des European Privacy Seal (EuroPriSe) durchgeführt. Ziel ist es, die Re-Zertifizierung für ProCampaign nach beiden Standards zu erlangen. Grundlage für die Auditierung ist daher einerseits die Version 2 des Anforderungskatalogs zum Datenschutz-Gütesiegel für IT-Produkte des ULD[4], andererseits der EuroPriSe-Kriterienkatalog in der Version von November 2011. Die Zusammenfassung der Ergebnisse der EuroPriSe-Evaluation bleiben einem gesonderten Bericht vorbehalten, der an anderer Stelle veröffentlicht ist[5].

Im Ergebnis stellen die Auditoren fest, dass ProCampaign in der Version 7.0 unter Beachtung der dem Anwender zur Verfügung gestellten Datenschutzhinweise weiterhin konform zu den gesetzlichen Anforderungen an den Datenschutz und die Datensicherheit eingesetzt werden kann und dass ProCampaign in der Standardausführung unter Beachtung der Datenschutz-Hinweise in besonderem Maße den Datenschutz beim Anwender fördert.

---

[1] Im Verfahren Nr. DE-110027 mit der Gültigkeit bis zum 28.02.2014.
[2] Im Verfahren Nr. 02-03/2012 mit Gültigkeit bis zum 06.03.2014.
[3] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, *GVOBl.* Schl.-H. *2013, S.536ff.* Sie ersetzt seit dem 01.01.2014 die Datenschutzauditverordnung.
[4] Weitere Informationen sind abrufbar unter https://www.datenschutzzentrum.de/.
[5] Abrufbar unter https://www.european-privacy-seal.eu. Diese sowie weitere genannte Webseiten waren mit Stand zum Februar 2017 online abrufbar.

2. Antragstellerin

Antragstellerin der Auditierung und Zertifizierung gemäß DSGVO 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.

3. Sachverständige Prüfstelle

Sachverständige Prüfstelle gemäß DSGVO 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 Begutachtung erstreckte sich auf den Zeitraum von 02.01.2014 bis 03.02.2017 und beinhaltete neben der konzeptionellen Analyse der von Consultix GmbH zur Verfügung gestellten Dokumente auch die Durchführung von Plausibilitätstests an der Anwendung sowie eine Besichtigung der Webseiten des Unternehmens unter https://www.consultix.net/ und des Rechenzentrums der Consultix GmbH am Standort in Bremen.

5. Kurzbezeichnung der Anwendung

Auditiert wurde das IT-Produkt ProCampaign in der Version 7.0 sowie der IT-basierende Service anhand des Funktionsstands vom Januar 2017.

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.

ProCampaign ist dabei grundsätzlich auch als Verwaltungssystem für Personendaten bei öffentlichen Stellen (z. B. im Bereich Tourismus oder Stadtmarketing) anwendbar, so dass eine Zertifizierung gemäß DSGSVO grundsätzlich in Betracht kommt.

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 an die Hand 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 angegebene 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.

ProCampaign besitzt eine separate Eingabemaske für ein Beschwerdemanagement, das sog. „ProComplaint“, für Kunden, die ihr Beschwerdemanagement über ein kundeneigenes Callcenter ebenfalls über ProCampaign führen. Insofern ist ProComplaint ein alternatives GUI zu ProCampaign mit eingeschränktem Funktionsumfang. Aus Gründen der Übersichtlichkeit für den Kunden wird dabei ProComplaint über eine eigene Domäne geführt. ProComplaint liegt innerhalb des Funktionsumfangs von ProCampaign und ist damit ebenfalls Auditgegenstand.

6.2 Funktionsumfang der auditierten Standardausführung

ProCampaign besitzt insbesondere folgende Funktionen:

--- Deduplication von Datensätzen (**unverändert ggü der Version 2.0**)

Eine integrierte Duplikaterkennung verhindert nach bestimmten Kriterien, dass Profile mehrfach in der ProCampaign Datenbank angelegt werden (= Profil-Duplikat: Dieselbe Person ist in mehr als einem Profil gespeichert). Folgende Kriterien werden für die Duplikaterkennung genutzt:

- Vorname, Nachname, E-Mail-Adresse
- E-Mail-Adresse, Geburtsdatum
- Vorname, Nachname, PLZ, Straße

Es können auch noch weitere Kriterien definiert werden, um so den Prozess der Duplikaterkennung ggf. anzupassen.

--- Einrichtung und Verwaltung der Einwilligungserklärung des Konsumenten (**unverändert ggü der Version 2.0**)

Konsumenten, die ihre Zustimmung für die Zusendung von Mailings bzw. E-Mailings gegeben haben, erhalten einen Opt-In. Ein Konsument kann mehrere Opt-Ins besitzen, z. B. ein Opt-In für die Zusendung von Mailings per Post, ein Opt-In für die Zusendung von E-Mailings, aber auch ein Opt-In für die Informationsmitteilung per Telefon (SMS). Möchte ein Konsument etwa nicht mehr per Post kontaktiert werden, erhält er für diesen Kanal einen Opt-Out.

--- *Optional auf Wunsch des Kunden*: Postadressen-Check und Korrektur (**unverändert ggü der Version 2.0**)

Wird ein neues Profil mit einer Postadresse in der Datenbank angelegt, erfolgt ein Postadress-Check mit anschließender Korrektur der falschen Postadresse (sofern dieser Postadress-Check vom Anwender gewünscht ist). Sobald etwas an dieser Adresse geändert wird, wird der Postadress-Check erneut durchgeführt. Neben der postalischen Überprüfung wird auch eine Korrektur der Schreibweise vorgenommen. Die Korrektur wird vom System selbst vorgenommen, es werden keine Daten hierfür exportiert. Hierfür erwirbt die Consultix GmbH im Namen des Kunden eine Lizenz an einer anonymen Adressdatenbank, gegen die lokal geprüft wird. Der Abgleich der Daten umfasst ausschließlich die Adressdaten ohne den Namen des Konsumenten und wird offline durchgeführt.

Eine manuelle Auswahl von zu überprüfenden Adressen ist nicht vorgesehen.

Der Postadressen-Check gehört nicht zum Standard-Umfang von ProCampaign und ist daher auch nicht Auditgegenstand.

--- Vergabe von Registrierungsnummern (**unverändert ggü der Version 2.0**)

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 (z. B. bei Ausübung des Widerspruchsrechts oder bei Eintrag in die Robinsonliste) (**unverändert ggü der Version 2.0**)

Hat der Konsument in der Vergangenheit seine Zustimmung für die Zusendung von Informationen z. B. per E-Mail und per Post gegeben und widerspricht nun dieser Zustimmung, erhält er einen Opt-Out. Dadurch wird sichergestellt, dass er nicht mehr über diesen Kanal kontaktiert wird.

--- Datenbereinigung (**leicht verändert ggü der Version 2.0**)

Kann ein Newsletter nicht zugestellt werden, wird dieser Umstand per E-Mail an ProCampaign rückübermittelt. Diese unverschlüsselte E-Mail enthält als personenbezogenes Datum die E-Mail-Adresse des Konsumenten. Profile, bei denen Newsletter wiederholt nicht ankommen,

sollen automatisch nach einer gewissen Zeit gelöscht werden (d. h. Profile mit 3 Bounces). Auch Profile, die inaktiv sind, d.h. für die 18 Monate (**zuvor in der Version 2.0 noch 24 Monate, dies wurde mit der Version 7.0 reduziert**) keinerlei Transaktionen (z. B. Gewinnspielteilnahme, Newsletter-Response) gemeldet wurden, werden gelöscht. Da diese Profile in Statistiken vorkommen, erfolgt eine mehrstufige Löschung der Daten. Im ersten Schritt werden die Opt-Ins der Profile entfernt. Im zweiten Schritt werden diejenigen Profile, die 6 Monate keinerlei Permission (Einwilligung) mehr haben, als gelöscht markiert. Einen Monat später werden die personenbezogenen Attribute entfernt (ein Personenbezug ist also nicht mehr herstellbar), 48 Monate später werden alle Transaktionen gelöscht.

Offline Rückläufer (d. h. ein Mailing per Post ist nicht beim Empfänger angekommen) gelangen auf eine separate Liste, damit die Daten in ProCampaign entsprechend gepflegt werden können.

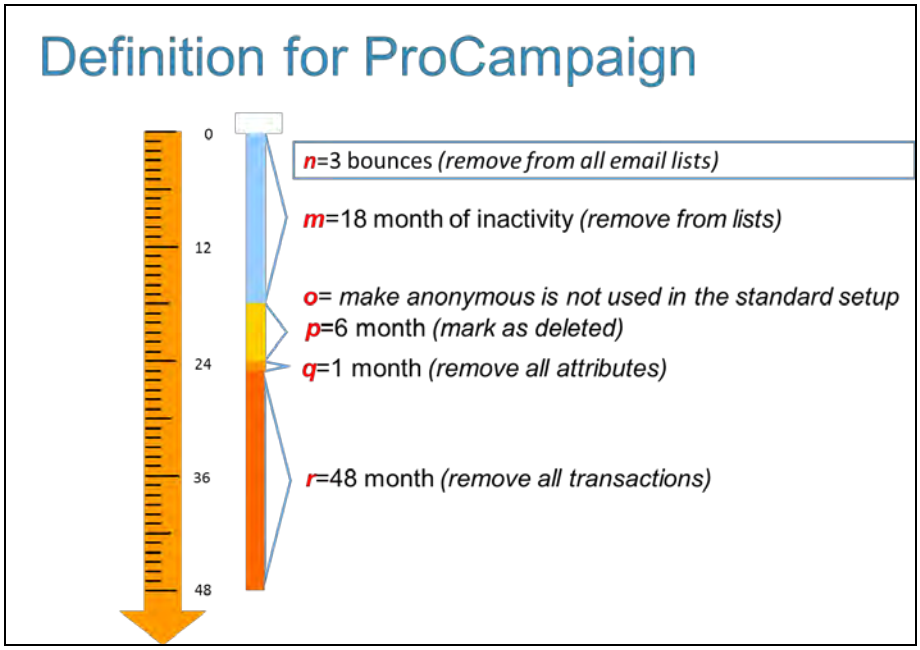

Abbildung 1: Cleanup-Prozess bei ProCampaign

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

Im IPS werden ausschließlich auffällige, als Angriff identifizierte IP-Adressen gespeichert. Als Angreifer identifizierte IP-Adressen werden in Quarantäne verschoben.

Die IP-Adressen im Netflow_Log werden spätestens nach 24 Stunden anonymisiert, indem die zwei letzten Oktette gelöscht werden. Die Logdateien werden nach 12 Monaten gelöscht.

Logfiles des Web-Servers der XML-API werden nach 7 Tagen gelöscht. Sie werden ausschließlich auf Antrag bei Beschwerden ausgewertet. In den Logfiles werden nur Aktionen von Konsumenten protokolliert, die

eine Einwilligung zur Speicherung ihrer Daten gegeben haben und deren Daten in der Datenbank gespeichert sind. Das Löschen nach 7 Tagen wird als angemessen bewertet.

Logfiles des https Web-Servers (GUI-Servers) werden nach 12 Monaten gelöscht, da Consultix GmbH dem Anwender gegenüber vertraglich im ASP-Vertrag verpflichtet ist, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle sowie Protokollierung von Changes). Bei einer kürzeren Speicherdauer müsste Consultix sich von der Nachweispflicht entbinden lassen.

Das Audit-Log zeichnet nur die IP-Adressen der Consultix-Systeme auf, die ein Ereignis generieren, bei Konsumenten-Tätigkeiten also die IP-Adresse der XML-API. Die Speicherung der Konsumenten-IP findet nur im Datenbereich des Logs statt, in dem die personenbezogenen Daten des Konsumenten, für die es entsprechend eine Einwilligung gibt und die in der entsprechenden Transaktion erfasst worden sind, gespeichert werden. Das Audit-Log wird nach 6 Monaten gelöscht.

Die Log-Daten für die administrativen Zugriffe auf die Datenbank werden ebenfalls nach einem Jahr gelöscht. Auch hier greift die vertragliche Nachweispflicht gegenüber dem Kunden.

--- *Optional auf Wunsch des Kunden:* Mover Check

Für diese Rückläufer kann zusätzlich ein Mover-Check durchgeführt werden, um ggf. neue Adressen durch Umzug in Erfahrung zu bringen (**unverändert ggü der Version 2.0**). Hierfür werden Daten im Auftrag des Kunden an einen anderen Dienstleister durch Medienbruch (also nicht automatisiert über ProCampaign) weitergegeben (i.d.R. an die Referenzdatenbank der Deutschen Post in Form einer Tabelle). Die aktuellen Daten können dann über das DataEntryCenter wieder in ProCampaign eingepflegt werden. Der Mover-Check muss separat beauftragt werden und ist nicht im Standard-Umfang von ProCampaign enthalten. Diese Funktion gehört insofern auch nicht zum Auditgegenstand.

--- *Optional auf Wunsch des Kunden*: Ermittlung und Aufklärung von Verstößen gegen die jeweiligen Teilnahmebedingungen des Kunden im Rahmen von unerlaubten Mehrfachregistrierungen oder durch Gutschein-/ Coupon-Betrug (**unverändert ggü der Version 2.0**).

Diese Datenverarbeitung hängt von den jeweiligen Teilnahmebedingungen einer Marketing-Aktion des Kunden gegenüber den teilnehmenden Konsumenten ab. Nimmt ein Konsument an einer Marketing-Aktion teil, werden die Teilnehmerdaten in ProCampaign importiert und durchlaufen einen Prüfungsprozess. Hierbei wird zunächst anhand der individuell gegebenen Teilnahmebedingungen im Falle einer Altersbegrenzung (z. B. Gewinnspielteilnahme erst ab 18 Jahren; Newsletter-Abonnement erst ab 16. Jahren usw.) ermittelt, ob eine

Teilnahme valide ist oder nicht (Altersabgleich anhand des Geburtsjahres). Sodann wird – sofern es der Kunde bzw. dessen Teilnahmebedingungen vorsehen – geprüft, ob eine unerlaubte mehrfache Teilnahme vorliegt. Grundlage für diese Prüfung sind die Transaktionen zu einem Konsumentendatensatz in ProCampaign (Prüfung, ob bereits eine Teilnahme-Transaktion vorliegt). Sehen die Kunden in den Teilnahmebedingungen außerdem vor, dass nur Konsumenten mit einem deutschen Wohnsitz teilnehmen dürfen, findet ein Abgleich über die im System hinterlegten möglichen Postleitzahl in der BRD statt.

Diese Ermittlungsfunktionen gehören nicht zum Standard-Umfang von ProCampaign und sind daher auch nicht Auditgegenstand.

--- Auswertung und Ressourcenanalyse (**unverändert ggü der Version 2.0**)

Mit ProCampaign können individuelle Auswertungen für einzelne Mailings und andere Marketing-Aktionen erstellt werden (z. B. Gesamtsumme Teilnehmerzahl, Auswertung von Umfragen). Diese Analysen können sich auch auf personenbezogene Daten beziehen, z. B. „Wie viele der Teilnehmer stammen aus der Stadt X?“, „Wie viele der Teilnehmer sind X Jahre alt?“ usw.

--- *Optional auf Wunsch des Kunden:* Ermittlung des „Most Valuable Consumers“

ProCampaign stellt hierfür die technische Möglichkeit zur Verfügung, Algorithmen für die Berechnung von Zuständen zu hinterlegen (***unverändert ggü der Version 2.0***). Diese Algorithmen werden durch den Auftraggeber an Consultix zur Implementierung übergeben und von Consultix in ProCampaign implementiert. Die Nutzung dieser Information wird vom Kunden individuell veranlasst und gehört nicht zum Standardumfang von ProCampaign. Es ist daher auch nicht Auditgegenstand.

--- *Optional auf Wunsch des Kunden*: Name-Check und Korrektur (**unverändert ggü der Version 2.0**)

Wird ein neues Profil in der Datenbank angelegt, erfolgt ein automatischer Name-Check (sofern dieser Name-Check vom Anwender gewünscht ist). Sobald etwas am Namen geändert wird, wird der Name-Check erneut durchgeführt. Anhand einer in ProCampaign integrierten Vornamens-Datenbank wird der Vorname an sich geprüft und ob das Geschlecht und die Anrede des Profils korrekt angegeben wurden. Darüber hinaus wird auch eine Korrektur der Schreibweise vorgenommen. Für die Korrektur werden keine Daten aus dem System exportiert. Die Abgleichdatenbank wurde von Consultix GmbH selber generiert. Daten werden nur korrigiert bei einer Sicherheit von über 90 %, dass ein Fehler vorliegt.

Der Name-Check gehört nicht zum Standard-Umfang von ProCampaign und ist daher auch nicht Auditgegenstand.

--- Datenselektionen (**unverändert ggü der Version 2.0**)

Eine Datenselektion ermöglicht es dem Anwender, offline oder online Mailings zielgerichtet an spezifische Zielgruppen zu adressieren. Ziel ist es, Streuverluste möglichst zu mindern. Anhand von bestimmten Kriterien werden diese Zielgruppen aus dem Datenbestand selektiert.

--- ProComplaint (**unverändert ggü der Version 2.0**)

ProComplaint ermöglicht einen begrenzten Datenbankzugriff auf die Konsumenten-Daten durch ein Call-Center. Bei Konsumentenanfragen können die Call-Center Agents anhand der aufgeführten Transaktionen Auskunft geben (z. B. Anfragen zu Aktions-Teilnahmen). Darüber hinaus ist es möglich, Daten direkt in ProCampaign zu ändern, da ProComplaint über dieselbe Schnittstelle auf die ProCampaign-Datenbank zugreift. Außerdem ist es möglich, auf Wunsch eines Konsumenten dessen personenbezogene Daten anzugeben (Auskunftsersuchen). Besteht ein Konsument auf die Auskunft über sämtliche über ihn gespeicherte Daten, wird die Anfrage an die Consultix GmbH weitergeleitet. Die Consultix GmbH erstellt dann einen vollständigen Profil-Auszug aus ProCampaign und sendet dies dem Konsumenten zu. Ebenfalls ist es im Rahmen von ProComplaint möglich, Konsumentendaten auf Anfrage zu löschen. Hierzu verwendet der Call-Center-Mitarbeiter den „delete Profile"-button, wodurch das Profil als gelöscht markiert wird (Datensperrung), woraufhin vom Anwender nicht mehr darauf zugegriffen werden kann. Beim nächsten Löschzyklus werden die Daten endgültig gelöscht. Der Prozess der Identifizierung/Verifizierung eines Konsumenten durch den Agenten wird vom jeweiligen Anwender definiert und kann mittels ProComplaint nicht unterstützt werden.

Folgende Funktionen sind in der Version 6.0 von ProCampaign neu bzw. erweitert worden:

--- **Umfragen (neu mit Version 6.0)**

ProCampaign bietet die Möglichkeit dynamische Formulare für Konsumentenumfragen auf Webseiten zu definieren (Funktion „Umfragen"). Hinter den „Umfragen" steht eine Formular-Generierungsfunktion, mit der in ProCampaign Formulare definiert werden können. Hier können Fragen für die Umfragen und Muster-Attribute, wie Vorname, Nachname, E-Mailadresse in einem Formular als Feld definiert werden. Der Konsument füllt dann das Formular aus. Wie bei normalen Formularen, die über APIs in ProCampaign einlaufen, werden die Antworten der Konsumenten in der Funktion Attribute gespeichert.

Die hierzu vorhandene Bezeichnung der „Estimated Acceptance" hängt mit der Dynamisierung der Fragen zusammen. Dabei können die Formulare so konfiguriert werden, dass bei einer Umfrage nur bestimmte Fragen aufklappen und andere gar nicht oder nicht sofort. Die „Estimated Acceptance" dient hierbei der Priorisierung von Daten-Feldern in dem Umfrageformular. Der Anwender setzt hierbei die Prioritäten für die einzelnen Fragen und legt diese z. B. anhand einer Prozentzahl oder

anhand eines selbstdefinierten Bewertungsmaßstabs fest. Bei der Konfiguration des Umfrageformulars setzt der Anwender nun die von ihm selbst definierten Werte pro Frage bzw. Daten-Feld fest. Dieser Wert gibt die Einschätzung des Anwenders wieder, in wie weit der Konsument wahrscheinlich bereit ist, die Frage zu beantworten. Anhand der verschiedenen hinterlegten Werte wird dann die Reihenfolge der Daten-Felder bzw. Fragen hinterlegt. Die Funktion des „Estimated Acceptance" ist demnach kein personenbeziehbares Datum, sondern nur ein Wert zur Bestimmung einer Reihenfolge von Daten-Feldern.

--- **Messaging (erweitert mit Version 6.0)**

Das Messaging bezeichnet den ehemaligen Bereich „E-Mailings" (E-Mail-Versand) und meint nunmehr den Versand von E-Mails und SMS (neu) an Konsumenten.

Das Versenden per SMS funktioniert genauso wie das Versenden einer E-Mail. Der einzige Unterschied ist, dass der Anbieter hier den gewünschten SMS-Provider hinterlegen muss, über den die SMS versandt werden. Die Consultix GmbH übermittelt dabei Absendernummer (alphanumerisch, in der Regel ist dies der Markenname des Kunden), die Zielrufnummer des Konsumenten sowie den SMS-Text über eine Schnittstelle per https an den vom Anwender/Kunden vorgegebenen Provider. ProCampaign liefert insofern nur die Daten für das SMS-Messaging an den Provider. Die eigentliche Telekommunikation erfolgt über den vom Anwender/Kunden vorgegebenen Provider und ist nicht Gegenstand des Audits.

--- **Multivariates Testing (neu mit Version 6.0)**

ProCampaign ermöglicht es, vor Versand eines E-Mail-Newsletters an einen Konsumenten einen multivariaten Test durchzuführen. Dabei werden verschiedene Varianten des Newsletters erstellt. Jede Variante wird als Stichprobe an einen kleineren Empfängerkreis gesendet. Nach dem Versand wird geprüft, welche Variante die besten Ergebnisse an Clicks and Opens oder an einer bestimmten Transaktion (z. B. Teilnahme an einem Gewinnspiel) hatte. Clicks ist das Anklicken eines Links im Newsletter, Opens ist das Herunterladen von Zählpixeln in Bildern in Newslettern. Das Tracking erfolgt dabei unabhängig von der IP-Adresse des Konsumenten. Über ProCampaign werden hingegen keine Cookies gesetzt. Der Rest der Konsumenten auf der Empfängerliste erhält im Anschluss die beste Variante. Dabei kann die beste Variante manuell vom Anwender oder automatisch von ProCampaign nach den zuvor eingegebenen Kriterien versandt werden. Zur Bildung der Stichprobe wird eine Untermenge von Daten gleichverteilt aus der gesamten Datenbank entnommen. Dabei werden die Profile nicht nach personenbezogenen Daten ausgewählt, sondern nach mathematischen Berechnungen (Verfahren: „Klumpen-Stichprobe"). Die Klumpen-Stichprobe ist ein anerkanntes mathematisches Verfahren für die Zufallsauswahl. Es kommt hierbei nicht auf den einzelnen Konsumenten an, sondern auf alle Konsumentenprofile, die in einem „Klumpen" geclustert sind. Die

Ergebnisse dieses Tests lassen keine personenbeziehbaren Rückschlüsse zu, sondern nur statistische Werte, anhand derer die Auswahl der besten Newsletter-Variante dargestellt wird.

--- **Best Send Time Optimization (neu mit Version 6.0**)

Diese Funktion erlaubt es, E-Mails für jeden Konsumenten zu einer individuell bestimmten, optimalen Zeit zu versenden. Der beste Zeitpunkt wird anhand der Zeitpunkte der Clicks and Opens des Konsumenten in vorherigen Nachrichten berechnet. Diese Erfassung/Auswertung der Clicks und Opens erfolgt nur nach Einwilligung des Betroffenen.

--- **Link Tagging (neu mit Version 6.0)**

Die Funktion des Link Tagging ermöglicht dem Anwender, alle Links einer E-Mail anhand von Tags zu kategorisieren. Diese Kategorisierung erlaubt eine aggregierte Sicht auf die Daten. Die Tags können zu Auswertungszwecken im Zeitverlauf betrachtet und im Nachhinein für die gezielte Ansprache der Konsumenten verwendet werden (z. B. Versand eines Newsletters an alle Konsumenten, welche die Links einer Kategorie mindestens 3mal geklickt haben).

--- **Statistics (neu mit Version 6.0)**

Im Bereich Statistics hat der Anwender Zugriff auf aggregierte Konsumentendaten. Hier ist es möglich, Statistiken über einen Zeitverlauf zu betrachten (z. B. Registrierungen für einen Newsletter in einem bestimmten Monat, Teilnahmezahlen an einem Gewinnspiel). Über diese Funktion können bestimmte generelle und nicht personenbeziehbare Indikatoren für die Erstellung der Statistik ausgewählt werden. Es erfolgt dann eine graphische Übersicht der Anzahl aller zutreffenden Profile und E-Mails im Zeitverlauf. In der Bearbeitungsmaske wird diese Grafik dargestellt, wobei kein Bezug auf einzelne Profile erfolgt, sondern nur eine kumulierte Auswertung im zeitlichen Verlauf. Die Auswertungen im Bereich Statistics sind daher nicht direkt einer natürlichen Person zuzuordnen. Allerdings ist es möglich, anhand der Statistiken z. B. ein bestimmtes Gewinnspiel zu betrachten und sich dann hierzu die Daten der Teilnehmer aus ProCampaign über die Bearbeitungsmaske zu diesem bestimmten Gewinnspiel herauszusuchen. Insofern liegt keine anonymisierte Auswertung vor.

--- **Direct Query (neu mit Version 6.0**)

Mit dem Direct Query können eingeschränkt SQL-Abfragen auf der Datenbank direkt vom Anwender durchgeführt werden. Die Abfragen beschränken sich auf E-Mailings für die Open und Clicks, bei Couponaktionen auf die Einlösung der Coupons und bei Transaktionen (z. B. Gewinnspielen) auf die Teilnahme. Ferner können nur SQL-Abfragen über Alter, Anzahl der Kinder im Haushalt, Geschlecht und Haushaltsgröße abgefragt werden.

Die Abfragen beziehen alle für die Abfrageparamenter zutreffenden Profile ein. Als Ergebnis der Abfrage, in welche maximal 1.000 Profile einbezogen werden können, wird eine Zahl dargestellt, nicht aber das

Profil eines Konsumenten. Diese Zahl ist ein sogenannter „Count“ und stellt als Ergebnis dar, wie viele Treffer ein Direct Query mit den durchgeführten Parametern ergeben hat.

Im Direct Query gibt es demnach keinen Zugriff auf personenbezogene Daten eines einzelnen Konsumenten. Auch ist ein Rückschluss über die für das Konsumentenprofil ausgegebene „Entity ID“ nicht möglich. Die „Entity_ID“ ist eine interne ID und lässt sich nicht in der Profilsuche verwenden.

Theoretisch ist es allerdings möglich, dass ein berechtigter Anwender die Suche anhand aller genannten Parameter so eingrenzt, dass nur ein oder wenige Counts angezeigt werden und er nun – sofern er für den Zugriff auf einzelne Profile denn eine systemseitige Berechtigung erhalten hat – über eine Transaktions-Nummer die zutreffenden Profile aus der Datenbank heraussucht. Da nur Daten ausgewertet werden, für die der Anwender eine Einwilligung des Konsumenten eingeholt hat, für den der Suchende eine Berechtigung zugewiesen bekommen hat und der Anwender das Berechtigungskonzept prüfen und pflegen muss, ist dies unkritisch. Der Anwender wird darauf sensibilisiert, durch organisatorische Maßnahmen (z. B. durch eine Betriebsanweisung) einer Nutzung der Direct-Query-Funktion, welche die Ermittlung individueller Profile zum Ziel hat, entgegen zu wirken und die Abfrageprotokolle regelmäßig zu kontrollieren, um eine missbräuchliche Nutzung zu verhindern.

--- **Couponing (neu mit Version 6.0 und 7.0)**

Der Anwender kann mit ProCampaign Couponing-Aktivitäten für Konsumenten definieren. Hierbei können z. B. bestimmte Coupons einer bestimmten Konsumentenprofilgruppe zugeordnet werden (z. B. Coupons für T-Shirts für Herren und Damen). Die Kriterien für ein Konsumentensegment, sowie den für dieses Segment geltenden Rabatt werden durch den Anwender definiert. Hierfür stehen alle vom Kunden definierten Attribute und das Konsumentenverhalten („behavior related data“) zur Verfügung. Das „behavior related data“ bezieht sich auf die Teilnahme an E-Mailings und Gewinnspiel-Transaktionen sowie Couponeinlösungen, die im Rahmen der Kundenbeziehung mit Einwilligung erhoben wurden.

In der Praxis wird die Segmentierung dazu genutzt, um herauszufinden, für welche Konsumentengruppe die Coupons interessant sind und um eine sogenannte Incentivierung von irrelevanten Coupons zu vermeiden. Beispiel: Windelcoupons sind nur interessant, wenn Kleinkinder im Haushalt leben. Hat der Konsument Angaben zu der Anzahl der Kinder in seinem Haushalt gemacht (mit Einwilligung / Permission), können diese Daten segmentiert werden.

Im Rahmen der Segmentierung kann der Anwender auch externe, also außerhalb von ProCampaign erfasste Daten, welche legitim mit einer Einwilligung / Permission erfasst wurden, nutzen und ProCampaign damit

anreichern. Ein Beispiel hierfür ist die Erweiterung um sogenannte Mosaik Daten. Dies sind im hiesigen Zusammenhang alle auf Postleitzahlen basierende statistische Informationen, die dann vom Anwender in ProCampaign übernommen und dort für eine Segmentierung genutzt werden könnten.

Der Anwender kann die Daten in die Standardausführung von ProCampaign einpflegen, dies obliegt jedoch seiner eigenen Verantwortung, Daher ist die Erfassung und Nutzung dieser externen Daten in ProCampaign ist nicht Gegenstand des Audits.

--- **Neu mit Version 7.0:** Über eine API Schnittstelle kann beim Couponing mit dem Systemaccount des Anwenders (z. B. Kassensystem, Shop-System) kommuniziert werden. In diesem Fall muss das dahinterliegende System die Nutzer-Berechtigungen verwalten und alle Vorgänge so protokollieren, dass der Nutzer mit Zeitstempel festgehalten wird, da es sich dann um für die Abrechnung (des Kassen- bzw. Shopsystems) finanzbuchhalterisch relevante Daten handelt. Das protokollierende, angebundene System ist allerdings nicht mehr Zertifizierungsgegenstand.

--- **Geolokalisation (neu mit Version 6.0)**

ProCampaign bietet die Möglichkeit, anhand der Postleitzahl eine regionale Auswahl zu erstellen, was als „Geolokalisation“ benannt ist. Folgende Unterfunktionen sind möglich:

- Anhand der Postleitzahl werden alle für eine Marketing-Aktion in Betracht kommenden und dafür freigegebenen Konsumentenprofile innerhalb von ProCampaign angezeigt. Anhand mehrerer Postleitzahlen können auch die am häufigsten frequentierten Postleitzahlen – bezogen auf vorhandene und freigegebene Profile in ProCampaign – ermittelt werden.
- Anhand der Postleitzahl und eines vom Anwender ausgewählten Radius von maximal 20km können vorhandene und dafür freigegebene Konsumentenprofile angezeigt werden (Der Bereich wird auch als „Profile Geocoordinates“ bezeichnet) - z. B. alle Profile innerhalb eines Umkreises von 20km um die Postleitzahl 28217.
- Anhand der Postleitzahl, eines vom Anwender ausgewählten Radius von maximal 20km sowie eines Standortes (z. B. eines Geschäfts) können innerhalb von ProCampaign vorhandene und dafür freigegebene Konsumentenprofile angezeigt werden (Der Bereich wird auch als „Shop Geocoordinates“ bezeichnet - z.B. alle Profile innerhalb eines Umkreises von 20km um die Postleitzahl 28217 und den Shop YY (Straße, Hausnummer des Shops).

Hervorzuheben ist, dass ProCampaign die Bezeichnung „Geolokalisation“ nicht im datenschutzrechtlichen Sinne einer Geolokalisierung verwendet. Es wird nicht erfasst, wo sich der Konsument aufhält oder ob er einen Shop bereits einmal besucht hat oder dort etwas gekauft hat. Vielmehr werden Postleitzahl, Radius und Shop-Koordinaten dazu genutzt, eine Selektion aus Konsumentendaten

des Anwenders zu ermöglichen, um diesen ausgewählten Konsumenten gezielte Informationen (Werbung) zukommen zu lassen. Beispiel: Teilnehmer am Nivea-Newsletter erhalten Informationen per E-Mail zu einer Shop-Eröffnung in Hamburg Mitte, wenn sie im Umkreis von 10km um den Shop wohnen und zuvor eingewilligt haben. Der Konsument wird auf die Verwendung seiner Postleitzahl zu Zwecken der individualisierten Werbung im Rahmen der jeweiligen Datenerfassung (z. B. Gewinnspielformular) hingewiesen und eine Einwilligung wird eingeholt.

Folgende Funktionen sind in der Version 7.0 von ProCampaign neu bzw. erweitert worden:

--- **Ratings & Reviews (neu mit Version 7.0)**

Mit dieser Funktion wird der Prozess von Produktbewertungen durch Konsumenten administriert und moderiert. Hierbei können Konsumenten Produkte (= Objekte) des Anwenders online bewerten oder kommentieren (= Review) und Bewertungsnoten abgeben (= ratings). Auch die Ratings und Reviews können wiederum beantwortet, bewertet oder benotet werden.

Über das Modul kann vom Moderator gesteuert werden, welche Ratings und Reviews veröffentlicht werden. Hierzu können Inhalte auch per Flag auf „Inapropriate“ gesetzt werden. Die Bezeichnung inaproproate bezieht sich auf eine interne Bewertung des Anwenders, dass dieser Beitrag nicht veröffentlicht werden darf. Usernamen sowie bestimmte Wörter des Beitrags können auf einer Blacklist gesperrt werden.

Das Modul Ratings & Reviews besteht aus einem Frontend (JavaScript Plugin Snippets) zur Visualisierung der Funktionen und Ergebnisse, einer REST API als Schnittstelle, Prozesslogiken, Konfigurationsmöglichkeiten und der Datenbank mit Export-/Import Funktion. Über das bekannte Rollen- und Berechtigungsmodel von ProCampaign können Verfasser, Moderatoren und Administratoren detailliert nach Berechtigungen und Rollen zugewiesen werden.

Ferner kann eine Benachrichtigungsfunktion per E-Mail eingerichtet werden, die über neue Ratings oder Reviews oder Änderungen informiert.

Die Reviews und Ratings werden über das jeweilige Webformular des Anwenders vom Konsumenten mit dessen informierter und jederzeit widerruflicher Einwilligung in ProCampaign erfasst und nach Überprüfung durch den Anwender auf dem Webportal veröffentlicht.

Ferner ist es möglich, dass der Konsument, der bereits einen Review oder ein Rating abgegeben hat, später per E-Mail über andere Produkte informiert wird (z. B. mit der Aufforderung, diese ebenfalls zu testen und zu bewerten). Hierbei wird das in ProCampaign bekannte Double-Opt-In-Verfahren angewendet.

Der Anwender wird im Datenschutzmerkblatt hinreichend auf die Einholung von Einwilligungen sensibilisiert. Ferner sind die datenschutzrechtlichen Anforderungen auch in einem

Datenschutzkonzept thematisiert. Danach muss der Konsument vor Datenerfassung über die konkrete Datenverwendung und sein Widerspruchsrecht informiert werden. Ferner ist zu beachten, dass die Veröffentlichung der Bewertungen durch den Konsumenten anonym oder zumindest unter einem Pseudonym ermöglicht und gefördert wird. Zudem sollte die Veröffentlichung der Bewertung von der Anerkennung von Nutzungsbedingungen abhängig gemacht werden, in denen verbindliche Regelungen zur Einhaltung einschlägiger Gesetze und Regelungen getroffen sind. Bei der Nutzung der Funktion Ratings & Reviews müssen daher die Beiträge *vor* der Veröffentlichung auf Rechtskonformität geprüft werden, was durch die Rolle des Moderators erfolgt.

--- **OAuth2-Schnittstelle (neu mit Version 7.0)**

ProCampaign bietet ab Version 7 alternativ zum bisherigen Verfahren per Benutzername und Passwort zusätzlich eine Authentisierungsschnittstelle auf der Basis von OAuth2 an, mit Hilfe derer Kunden von ProCampaign eine alternative Authentisierung realisieren können. Das bisherige Verfahren stellt die default-Einstellung für die Anmeldung dar. Bei Nutzung dieser Schnittstelle können sich Konsumenten über eine bereits vorhandene Authentisierung an einem anderen System für die Authentifizierung an dem von Ihnen gewünschten System anmelden. Ist z. B. in ProCampaign ein Konsumenten-Account auf einem Firmenportal hinterlegt, kann sich der Konsument auf Wunsch nun auch mit der Authentisierung an einem dazugehörigen Onlineshop registrieren. Sollte diese Funktion genutzt werden, muss der Konsument vor der Übermittlung seiner Daten an Dritte sowie über sein Widerspruchsrecht diesbezüglich und seine Rechte als Betroffener informiert sein und es ist eine Einwilligung in die Datenverarbeitung einzuholen. Zudem muss der Konsument über die für die Datenverarbeitung verantwortliche Stelle und über die damit verbundenen Sicherheitsrisiken aufgeklärt werden. Die Hinweise, welche Daten konkret ausgetauscht werden und welche Informationen die andere Stelle durch den Login erhält, sowie die Einwilligungserklärung müssen entsprechend vor einem Login eingebunden werden. Ebenso ist ein Hinweis in der Datenschutzerklärung auf den Webseiten notwendig. Nach deutschem Telemedienrecht ist es ferner notwendig, eine Nutzung anonym oder unter Angabe eines Pseudonyms zu ermöglichen.

--- ***Optional auf Wunsch des Kunden:*** **Eigene Definition des Double-Opt-In Workflows (neu mit Version 7.0**)

ProCampaign sieht das Double-Opt-In-Verfahren in einem zeitlich festgelegten Ablaufprozess vor. Diese Standardkonfiguration kann der Anwender allerdings auch ändern und nach seinen Wünschen definieren. Dabei müssen die rechtlichen Anforderungen an das Double-Opt-In eingehalten werden.

Die Datenerfassung beim Anwender und Konsumenten, alle über den IT-Service bzgl. ProCampaign hinausgehenden Dienstleistungen der Consultix GmbH, die Einsatzumgebung beim Anwender, Konsumenten und Fullfilment-Partner sowie die

Abrechnungsprozesse zwischen der Consultix GmbH und dem Anwender gehören jedoch nicht zum Funktionsumfang 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:

- --- Postadressen-Check und Postadressenkorrektur
- --- Mover-Check und -korrektur
- --- Name-Check und-korrektur
- --- die Ermittlung des „Most Valuable Consumer“
- --- die Einbindung des Providers beim neuen SMS-Versand und deren IT-Umgebung ab der Version 6.0 von ProCampaign.
- --- Ebenso gehören die mit der Version 7.0 von ProCampaign neu eingeführten Funktionen eines Workflowmanagements für Double-Opt-In E-Mailings nicht zum Standardumfang, sofern der Anwender diese für seine Zwecke abweichend konfiguriert.
- --- Die Anreicherung von ProCampaign mit externen, also außerhalb von ProCampaign erfassten Daten, gehört nicht zum nicht Auditgegenstand. Insbesondere die für das Couponing nutzbaren externen Mosaik Daten sind nicht Gegenstand des Audits.
- --- Consultix bietet seinen Kunden Java Script Snippets an, um die API im Rahmen von Ratings & Reviews anzusprechen. Diese stellen nur ein Angebot an den Kunden dar und sind weder verpflichtend zu verwenden, noch gehören sie zum zertifizierten Scope des ToE.
- --- Neben der Standardmethode zur Authentisierung an ProCampaign per Benutzername und Passwort, unterstützt ProCampaign auch die Anmeldung über SingleSignOn-Dienste.

Ebenfalls nicht zum ToE gehören

- --- die Datenverarbeitung beim Anwender von ProCampaign
- --- alle über den IT-Service bzgl. ProCampaign hinausgehenden Dienstleistungen der Consultix GmbH
- --- die Einsatzumgebung beim Anwender, Konsumenten und Fullfilment-Partner, z.B. am PC oder Tablettsdie Abrechnungsprozesse zwischen der Consultix GmbH und dem Anwender.

Ebenfalls nicht Gegenstand der Evaluierung sind die über ProCampaign einbindbaren Medien (insbesondere Webseiten, Callcenter) des Anwenders.

7. Modellierung des Datenflusses

Mittels ProCampaign werden sowohl Primärdaten als auch Sekundärdaten verarbeitet.

7.1 Primärdaten

- --- **Unverändert**: Hierzu gehören personenbezogene oder –beziehbare Daten des Konsumenten, die dieser anhand der vom Anwender

definierten Datenfelder erfasst und die an die Datenbank von ProCampaign übermittelt werden. Dies sind in der Standarddefinition der Attribute: Name, Postadresse, Geburtsdatum. Weitere (ggf. personenbezogene oder –beziehbare) Attribute können vom Anwender hinzu definiert werden. Dies sind oftmals Telefonnummer, Handynummer, Faxnummer oder die E-Mail-Adresse.

--- **Neu: Soweit die neue Funktion der Geolokalisierung genutzt wird, gehören zu den Primärdaten zudem die Postleitzahl und die Postanschrift sowie der dazugehörige Radius eines Konsumentenstandorts.**

--- **Unverändert:** Hierzu gehören auch personenbezogene Daten, die als Kommentar in einem Freitextfeld im Rahmen des Beschwerdemanagements über ProComplaint in ProCampaign eingegeben werden könnten. In der Regel bezieht sich ein Kommentar aber auf einen Geschäftsvorgang, nicht auf eine Person. Letzteres kann jedoch nicht ausgeschlossen werden. Gleichwohl wird der Anwender auf den restriktiven Umgang mit Freitextfeldern sensibilisiert.

--- **Neu: Soweit die vom Anwender für die neue Funktion der Umfragen definierten Felder personenbezogene Daten enthalten oder Rückschlüsse auf eine natürliche Person zulassen, sind auch sie den Primärdaten zuzuordnen.**

--- **Unverändert**: Ebenfalls hierzu gehören die o.g. Registrierungsnummer eines Konsumenten (sog. Customer-ID) sowie Daten der jeweiligen Transaktion eines Konsumenten mit einem dazugehörigen Attribut, wie etwa die Bezeichnung als Teilnehmer für eine Aktion (Gewinnspielteilnehmer, Produkttester etc.). Transaktionsdaten sind allerdings ohne Attribute nicht personenbeziehbar.

--- **Unverändert**: Ferner gehört dazu das Nutzerverhalten anhand der „Clicks“ und „Opens“ in einem abonnierten Newsletter, die mithilfe eines Verschlüsselungs-Codes im Newsletter-Link erfasst werden (dieser Code enthält Angaben darüber, um welchen Konsumenten es sich handelt, um welchen Newsletter und um welches angeklickte Element).

--- **Unverändert:** *Es* gehört auch die IP-Adresse zu den Primärdaten, die zu dem Anschluss gehören, über den ein Konsument Daten an ProCampaign übermittelt.

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:

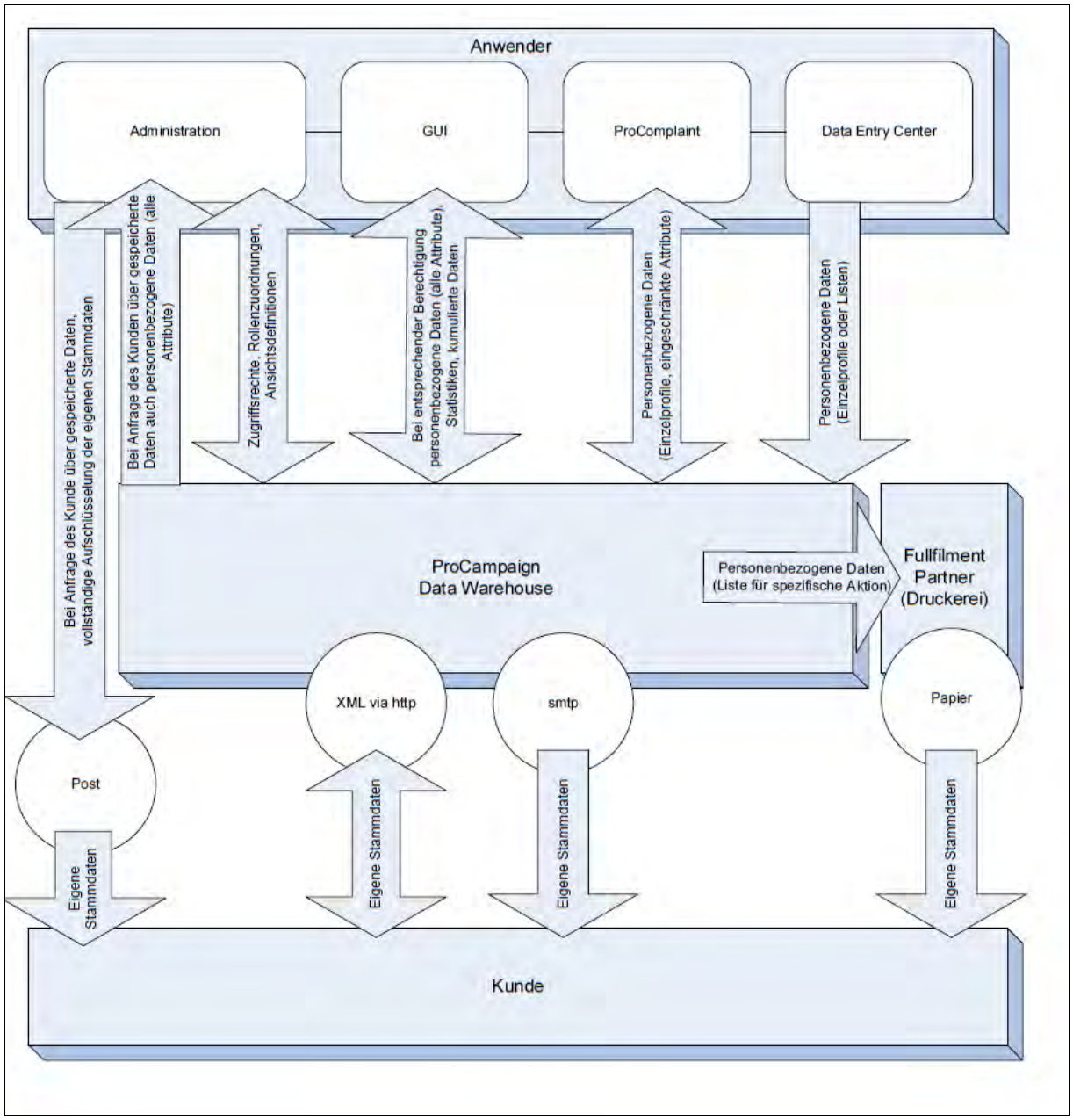

Abbildung 2: Datenfluss von ProCampaign

8. Eingesetzte Tools

Leicht verändert in Version 6.0. Sämtliche IT-Systeme werden durch mehrere Monitoring-Tools überwacht. Bei Unregelmäßigkeiten werden die Administratoren per SMS, E-Mail oder visuellen Hinweis informiert. Weiterhin werden alle Tätigkeiten auf den IT-Systemen protokolliert und können gegebenenfalls einzelnen Personen zugewiesen werden.

Das Netzwerk-Monitoring erfolgt auf verschiedenen Ebenen:

--- WhatsUp Gold dient zur Überwachung der Hardware (CPU-Last, Festplattenkapazität, Arbeitsspeicherauslastung) und Serverdienste.

Zwei zusätzliche Bildschirme in den Räumen der Administratoren sind installiert,

--- Traffic Monitoring erfolgt zur Überwachung der Bandbreite auf den Routern (**nun in der Version 6.0 Whatsup Gold anstelle von 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 Monitoringtools, wird die Sicherheit sämtlicher Daten, d.h. sowohl der Primär- aber auch der Sekundärdaten, also der Log-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 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

Hervorzuheben ist, dass die Consultix GmbH seit der letzten Zertifizierung von ProCampaign zudem ein Informationssicherheitsmanagementsystem für den Geltungsbereich „Data Center Services, Software & Website Development, Customer Relationship Management & Marketing Services“ vorweisen kann, welches gemäß ISO/IEC 27001:2013 zertifiziert wurde. Die Consultix GmbH ist bei der datenschutz cert GmbH unter der Zertifikats-ID: DSC.323.06.2015 erfolgreich gemäß ISO/IEC 27001:2013 zertifiziert. Das Zertifikat ist gültig bis zum 28.06.2018.

Die Server werden in einem Rechenzentrum in Bremen, Deutschland, mit starken Zugangs- und Zugriffskontrollen betrieben. Sämtliche Datentransfers mit ProCampaign werden verschlüsselt 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 konnten die Auditoren folgende Bewertungen treffen:

Nr.	Anforderungen	Bewertung	
A Allgemeines Anforderungsprofil (Primärdaten)			
	Komplex 1		
A1	1.1 Verfügbarkeit, Integrität, Vertraulichkeit	**adäquat**	
A2	1.2 Nicht-Verkettbarkeit	**adäquat**	
A3	1.3 Transparenz	**vorbildlich**	
A4	1.4 Intervenierbarkeit	**adäquat**	
A5	1.5 Anpassung des IT-Produkts	**adäquat**	

A6	1.6 Privacy by Default	**adäquat**	
A7	1.7 Sonstige Anforderungen	**n.a.**	
	Komplex 2		
A8	2.1 Ermächtigungsgrundlage	**adäquat**	
	2.1.1 Gesetzliche Ermächtigung	**adäquat**	
	2.1.2 Einwilligung des Betroffenen	**vorbildlich**	
	2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung	**adäquat**	
	2.1.3.1 Vorschriften über die Datenerhebung	**adäquat**	
	2.1.3.2 Vorschriften über die Übermittlung	**adäquat**	
	2.1.3.3 Löschung nach Wegfall des Erfordernisses	**adäquat**	
A9	2.2 Einhaltung allg. Datenschutzgrundsätze und Pflichten	**adäquat**	
	2.2.1 Zweckbindung und Zweckänderung	**adäquat**	
	2.2.2 Erleichterung der Umsetzung des Trennungsgebots	**adäquat**	
	2.2.3 Gewährleistung der Datensicherheit	**adäquat**	
A10	2.3 Datenverarbeitung im Auftrag	**vorbildlich**	
A11	2.4 Voraussetzungen besonderer technischer Verfahren	**n.a.**	
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	**n.a.**	
	2.4.2 Trennung der Verantwortlichkeiten	**n.a.**	
	2.4.3 Veröffentlichungen im Internet	**n.a.**	
	2.4.4 Weitere besondere technische Verfahren	**n.a.**	
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	**n.a.**	
A12	2.5 Sonstige Anforderungen	**n.a.**	
	2.5.1 Unterstützung Pseudonymität / Pseudonymisieren	**vorbildlich**	
	Komplex 3		
A13	3.1 Einzelne technisch-organisatorische Maßnahmen	**adäquat**	
	3.1.1 Physikalische Sicherung	**vorbildlich**	
	3.1.2 Authentisierung	**adäquat**	
	3.1.3 Autorisierung	**adäquat**	
	3.1.4 Protokollierung	**adäquat**	
	3.1.5 Verschlüsselung und Signatur	**adäquat**	
	3.1.6 Pseudonymisierung	**vorbildlich**	

	3.1.7 Anonymisierung	**adäquat**	
A14	3.2 Allgemeine Pflichten	**adäquat**	
	3.2.1 Technisch-Organisatorische Maßnahmen	**adäquat**	
	3.2.1.1 Verfügbarkeit	**adäquat**	
	3.2.1.2 Integrität	**vorbildlich**	
	3.2.1.3 Vertraulichkeit	**adäquat**	
	3.2.1.4 Nicht-Verkettbarkeit	**adäquat**	
	3.2.1.5 Transparenz	**vorbildlich**	
	3.2.1.6 Intervenierbarkeit	**adäquat**	
	3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	**vorbildlich**	
	3.2.1.8 Test und Freigabe	**vorbildlich**	
	3.2.2 Erleichterung der Vorabkontrolle	**adäquat**	
	3.2.3 Erleichterung der Erstellung von Verfahrensverzeichnissen	**adäquat**	
	3.2.4 Benachrichtigungspflicht	**adäquat**	
	3.2.5 Unterstützung behördlicher Datenschutzbeauftragter	**adäquat**	
A15	3.3 Spezifische Pflichten	**adäquat**	
	3.3.1 Verschlüsselung	**adäquat**	
	3.3.2 Anonymisierung oder Pseudonymisierung	**vorbildlich**	
	3.3.3 Spezielle Anforderungen bei besonderem Technikeinsatz	**n.a.**	
	3.3.3.1 Mobile Datenverarbeitungssysteme	**n.a.**	
	3.3.3.2 Video-Überwachung und –Aufzeichnung	**n.a.**	
	3.3.3.3 Automatisierte Einzelentscheidungen	**n.a.**	
	3.3.3.4 Veröffentlichungen im Internet	**n.a.**	
A16	3.4 Pflichten nach DSVO	**adäquat**	
A17	3.5 Anforderungen beim Betrieb der Auftragsdatenverarbeitung	**vorbildlich**	
A18	3.6 Sonstige Anforderungen	**n.a.**	
	Komplex 4		
A19	4.1Aufklärung und Benachrichtigung	**adäquat**	
A20	4.2Benachrichtigung bei unrechtmäßiger Kenntniserlangung	**adäquat**	

A21	4.3Auskunft	**adäquat**	
A22	4.4 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	**adäquat**	
	4.4.1 Berichtigung	**adäquat**	
	4.4.2 Vollständige Löschung	**adäquat**	
	4.4.3 Sperrung	**adäquat**	
	4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	**adäquat**	
	4.4.5 Gegendarstellung	**n.a.**	
A23	4.5 Sonstige Anforderungen	**n.a.**	
Nr.	Anforderungen nach Katalog oder sonstigen Rechtsnormen	Bewertung	
B Anforderungsprofil für Protokolldaten (Sekundärdaten):			
	Komplex		
B1	1.1 Datenvermeidung und Datensparsamkeit	**adäquat**	
B2	1.2 Zweckbindung	**adäquat**	
B3	1.3 Nicht-Verkettbarkeit	**adäquat**	
B4	1.4 Transparenz	**vorbildlich**	
	1.5 Sonstige Anforderungen	**n.a.**	
	Komplex 2		
B5	2.1 Rechtsgrundlagen	**adäquat**	
B6	2.2 Zweckbindung	**adäquat**	
B7	2.3 Aufbewahrungsfristen und Löschung	**adäquat**	
	2.4 Sonstige Anforderungen	**n.a.**	
	Komplex 3		
B8	3.1 Physikalische Sicherung	**vorbildlich**	
B9	3.2 Zugriffsschutz	**adäquat**	
B10	3.3 Ermittlung / Informationsgehalt	**adäquat**	
	3.4 Sichtbarkeit der Protokolldaten	**adäquat**	
B11	3.5 Technische Umsetzung der Speicherfristen	**adäquat**	
B12	3.6 Unzulässige Verkettung	**adäquat**	
B13	3.7 Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	**vorbildlich**	

	Sonstige Anforderungen	**n.a.**	
	Komplex 4		
B14	4.1 Selektive Löschung von Einzeldaten	**adäquat**	
	4.2 Beauskunftung	**adäquat**	
	4.3 Berichtigung	**adäquat**	
	4.4 Sperrung	**adäquat**	
	4.5 Einwand	**n.a.**	

11. Förderung des Datenschutzes

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

- --- Zentrale Komponente ist das gut strukturierte Einwilligungsmanagement als Basis für Marketingaktionen
- --- 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 7.0 sowie der dazugehörige IT-basierende Service mit Stand zum Januar 2017 erfüllen die Anforderungen an den Datenschutz und die Datensicherheit in besonderer Weise.

Bremen, den 03. Februar 2017

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

Ralf von Rahden
datenschutz cert GmbH