06/09 Juni

direkt marketing

Fachmagazin für modernes Direkt- und Dialogmarketing

Parteien im (Online-)Dialog

Wie Politiker heute Bürgernähe demonstrieren.

„Lessons Learned: Kontrolladressen wirkungsvoll im Einsatz“

Ein Beitrag von Dirk Niedernhöfer,
Geschäftsführer der adreko GmbH

www.direktmarketing.net

Lessons Learned: Kontrolladressen wirkungsvoll im Einsatz

Der Sommer 2008 wird in Deutschland die Direktmarketing-Praxis im Umgang mit personenbezogenen Daten nachhaltig verändern. Egal, wie die Novelle des Bundesdatenschutzgesetzes ausfallen wird und egal, ob Datenschutz-Audits vom Gesetzgeber vorgeschrieben werden oder nicht: Kunden, Nutzer und Partner aber auch Medien, Politik und Verbraucherschützer erwarten ein neues Verständnis von Datenschutz und eine neue Sensibilität im Umgang mit personenbezogenen Daten. Kontrolladressen-Systemen erhalten in diesem Zuge eine steigende Bedeutung.

Dirk Niedernhöfer

Kontrolladressen-Systeme gehören zu den Maßnahmen, mit denen Unternehmen und Dienstleister im neuen, den Datenschutz noch stärker in den Mittelpunkt rückenden Direktmarketing punkten können. Diese spezielle Form der Datensicherung ist außerhalb der Direktmarketing-Welt wenig bekannt und hat das Potenzial, Vertrauen zu schaffen. In einem, möglicherweise einmal Pflicht werdenden Datenschutz-Audit ist die Installation eines Kontrolladressen-Systems eine Maßnahme, mit der Werbungtreibende den Prüfer positiv überraschen können.

Allerdings fragt man sich mit Blick auf die 2008 gehäuft bekannt gewordenen Fälle von Adressen-Diebstählen, warum Kontrolladressen-Systeme hier nicht bereits im Vorfeld Alarm geschlagen haben. Im Fall der Adressen von Losinhabern diverser Lotterie-Einnehmer, die sogar mit Bankverbindung in Call Centern entwendet und im Markt angeboten wurden, scheint es definitiv zu illegalen Einsätzen gekommen zu sein. Ein professionelles System würde diese Einsätze aufdecken.

Somit bleiben zwei Möglichkeiten: Entweder die betroffenen Eigentümer der Adressen haben, sei es aus Unkenntnis heraus oder aus Kostengründen, auf den Einsatz von Kontrolladressen verzichtet. Oder die in den Adressbeständen eingesetzten Kontrolladressen haben den illegalen Einsatz nicht registriert – die Adressen haben also nicht mehr angeschlagen.

Das führt uns zu den „Lessons Learned“, die nach 2008 für Kontrolladressen-Systeme formuliert werden müssen.

Lesson Learned 1: Mehr Adressen-Sicherheit im Call Center

In nicht wenigen der bekannt gewordenen Daten-Diebstähle wurden Adressen in beauftragten Call Centern entwendet und im Markt angeboten – so auch im Fall der von Verbraucherschützern erworbenen CD mit den 6 Millionen Datensätzen. Datenschützer im Direktmarketing haben seit Jahren vor dem selbst gemachten Sicherheitsrisiko Call Center gewarnt. Durch den auf die Anbieter ausgeübten massiven Kostendruck werden Datenschutz-Konzepte Makulatur. Wenig Gehaltsspielraum und eng geschnürte Provisionsmodelle für Mitarbeiter, die oft ohne jede Kontrolle Zugriff auf Millionen wertvoller Datensätze haben, führen beinahe automatisch zum erhöhten Risiko eines Adress-Diebstahls.

Für die Zusammenarbeit mit Call Centern bedeutet das, die Datensicherheit als Leistungskriterium zu berücksichtigen – inklusive der Bereitschaft, für diese Leistung auch einen angemessenen Preis zu zahlen. Es bedeutet auch, Adress-Lieferungen an Call Center mit Kontrolladressen zu sichern. Missbrauch von Adressen im Call Center setzt nicht zwingend voraus, dass entwendete Daten auch telefonisch kontaktiert werden. Auf der anderen Seite ist klar, dass der Wert der Daten eben auch in der mitgeführten Rufnummer besteht. Gut beraten ist also, wer der Lieferung an das Call Center eindeutige Kontrolladressen mit einer überwachten Rufnummer zuspielt. So werden neben postalischen Kontakten auch telefonische aufgefangen und auf Rechtmäßigkeit geprüft.

Vorsicht: während im Bereich der Qualitätskontrollen das Mitschneiden und Auswerten von Anrufen ein effektives Mittel zum Zweck ist, das über entsprechende Ankündigungen und Passagen in den Mitarbeiter-Verträgen legitimiert werden kann, ist in der Datensicherung mittels Kontrolladressen-Rufnummern das Mitschneiden von Anrufen mit höchster Vorsicht zu behandeln!

In der Regel muss davon ausgegangen werden, dass mitgeschnittene Anrufe – auch, wenn sie einen Gesetzesverstoß des Anrufers dokumentieren – vor Gericht nicht als Beweismittel zugelassen werden. Im Gegenteil kann sich der Mitschneidende sogar strafbar machen. Auch, wenn der Mitschnitt in guter Absicht und zur Dokumentation eines Gesetzesverstoßes erfolgt ist! Alternativen sind die genaue Protokollierung von Anrufen sowie Aussagen der Mitarbeiter hinter den eingesetzten Rufnummern. Auch ist eine Protokollierung der anrufenden Nummern (soweit übermittelt!) ein nicht zu unterschätzendes Kriterium in der Dokumentation eines Adressenmissbrauchs.

Übrigens bieten der TÜV, aber auch andere Anbieter, eine Zertifizierung von Call Centern auch im Bereich Datensicherheit an.

Lesson Learned 2: Nachhaltigkeit des Kontrolladressen-Systems

Im Fall T-Mobile wurden Adressdaten 2006 offenbar intern entwendet und kursierten bis zum Bekanntwerden des Vorfalls 2008 im Markt. Während viele Anwender eines Kontrolladressen-Systems vom Direktmarketing-Grundsatz ausgehen, dass ein Adress-Datenbestand der älter als 12 Monate ist, nicht mehr aktuell ist und entsprechend auch nicht Gefahr läuft, illegal eingesetzt zu werden, lehrt uns die Datenschutz-Praxis etwas anderes: Hier werden Kontrolladressen durchaus auch Jahre nach dem eigentlichen Einsatz illegal kontaktiert. Was steckt dahinter? Ein älterer illegaler Datenbestand produziert durch die mittlerweile enthaltenen unbekannt Verzogenen und Verstorbenen eine höhere Retourenquote und damit höhere Kosten bzw. schwächeren Response. Dies relativiert sich durch geringere Aufwände für die Anschaffung gestohlener Adressen. Dazu kommt: systematisch illegal operierende Unternehmen rechnen damit, dass im Datenbestand enthaltene Kontrolladressen nach 12 Monaten oder mehr nicht mehr anschlagen. Oder dass durch eine fehlende Eindeutigkeit der Kontrolladressen ein illegaler Einsatz nach diesem Zeitraum nicht mehr nachgewiesen werden kann.

Für ein Kontrolladressen-System bedeutet das, dass der Nachhaltigkeit der Kontrolle eine besondere Bedeutung zukommt. Neben der Eindeutigkeit jeder eingesetzten Kontrolladresse – also der sicheren Zuordnung zu einer bestimmten Adresselektion und einem bestimmten Empfänger – liegt der Anspruch auch auf dauerhaft reagierenden Adressen. In einen Adressen-Bestand eingebrach-

Tipps für eine nachhaltige Kontrolle

- Auch Kontrolladressen sind Menschen: Neben Vertragsgestaltung und Incentivierung zählt die Motivation der Menschen hinter den Adressen. Informieren Sie über Erfolge und machen Sie den Sinn der gemeinsamen Arbeit transparent. So erreicht man eine hohe Beständigkeit.
- Kontrolladressen kontrollieren: Kontrollieren Sie Ihr Kontrolladressen-Panel laufend auf Zustellbarkeit und Zuverlässigkeit. Identifizieren und entfernen Sie schwarze Schafe und postalisch nicht mehr erreichbare Adressen so schnell wie möglich.
- Geizen Sie nicht mit Adressen: die Nachhaltigkeit der Kontrolle hängt auch von der Zahl der eingebrachten Kontrolladressen ab. Wenn Sie ohnehin nur 3 Kontrolladressen pro Adress-Selektion einbringen, steigt ihr Risiko, dass nach 12 Monaten keine der Adressen mehr aktiv ist. Berücksichtigen Sie neben der Größe der zu impfenden Adressdatei auch den Faktor Zeit und die gebotene Nachhaltigkeit der Kontrolle.
- Wenn Sie einen Dienstleister mit Ihrem Kontrolladressen-System beauftragt haben: wo nichts kommt (Kontrolladresse in einem nicht illegal verwendeten Adressenbestand), kann man auch nichts melden. Lassen Sie sich aber das Panel-Konzept erläutern und die Frage beantworten, wie der Dienstleister die Nachhaltigkeit seiner Kontrollen sicher stellt. ‹‹

te Kontrolladressen müssen mit hoher Wahrscheinlichkeit mittel- und langfristig aktiv und empfangsbereit bleiben. In der Praxis setzt das die entsprechende Pflege aber auch Kontrolle des eingesetzten Kontrolladressen-Panels voraus (vgl. Infokasten).

Lesson Learned 3: Sicherung gegen internen Missbrauch

Neben dem Daten-Diebstahl bei Dienstleistern standen 2008 auch wieder Zugriffe auf die Kunden-Datenbank innerhalb des eigenen Unternehmens im Vordergrund. Datenschützer mit Kontrolladressen-Background empfehlen seit jeher eine zweigleisige Sicherung:

Zum einen werden Adress-Selektionen, die Unternehmen verlassen, mit Kontrolladressen gesichert, um einen Missbrauch beim Empfänger gegebenenfalls aufzudecken und nachzuweisen. Kontrolladressen werden aber auch als echte Kunden in eine Kundendatenbank eingebracht und sind im Unternehmen selbst nur wenigen Eingeweihten bekannt. Diese Kontrolladressen schlagen auch nach einem Zugriff innerhalb des Unternehmens und dem Umgehen der üblichen Absicherungskanäle im Falle eines illegalen Einsatzes Alarm.

Man spricht in solchen Fällen auch von „Mystery Shoppern“ oder „Fake-Kunden“ – in diesem Fall nicht zu verwechseln mit den Testkäufern der Qualitätssicherung. Kontrolladressen sollten als Mystery Shopper immer wieder aktiviert werden, um eine lebendige Kundenhistorie zu erhalten und um in den für Datendiebe attraktivsten Selektionen vertreten zu sein (beispielsweise „Käufer letzte 6 Monate“). Oft werden eingebrachte Mystery Shopper unter dem Marketingleiter und dem Geschäftsführer eines Unternehmens aufgeteilt, so dass nicht ein Ansprechpartner allein alle Mystery Shopper einer Kundendatenbank kennt. Letzteres ist speziell im Falle eines Wechsels von Vorteil –wenn der Marketingleiter zum Mitbewerber wechselt.

Aufruf zur Kontrolladressen-Offensive

Das Direktmarketing musste im Zuge der Adressen-Diebstähle viel Kritik einstecken. In manchen Punkten war diese sicherlich berechtigt. An vielen Stellen stellt man aber lediglich wieder fest, wie schlecht das Image der Branche immer noch ist und wie wenig die Öffentlichkeit über die Grundregeln und das Grundverständnis im Direktmarketing informiert ist. Umso bedauerlicher, dass Datenschutz-Innovationen wie Kontrolladressen-Systeme und ihr Einsatz nicht offensiv angegangen und kommuniziert werden! In Diskussionen mit unterschiedlichen Gesprächspartnern kann man eine große Zustimmung zum Thema Kontrolladressen-System erleben – gerade auch aus den Reihen der schärfsten Kritiker. Eine Frage lässt sich allerdings dabei nicht beantworten: Wenn so eine sinnvolle Maßnahme im Direktmarketing entwickelt wurde und eingesetzt wird, warum spricht man dann eigentlich nicht darüber? dm