Praxisleitfaden E-Mail-Marketing
Datenkonzept und Zertifizierung im E-Mail-Marketing

Als größte Interessenvertretung der digitalen Wirtschaft begleitet der Bundesverband Digitale Wirtschaft (BVDW) e.V. das Thema E-Mail aktiv, um entwicklungshemmende Barrieren aus dem Weg zu räumen. Die Initiative E-Mail vereint Experten unter dem Dach des BVDW, die den Dialog zwischen E-Mail-(Service-)Providern, Dialogagenturen und E-Mail-Marketing betreibenden Unternehmern fördern. Sie verfolgt dabei einen ganzheitlichen Ansatz, der die drei Säulen E-Mail-Marketing, Servicekommunikation sowie Geschäftskommunikation umfasst. Als Metathemen behandelt die Initiative die spezifischen Felder Technik/Sicherheit, Marktzahlen und Messung, Recht, Internationalisierung, Standards und Daten. Dieses Whitepaper gibt einen Überblick zu rechtlichen Grundlagen, Datenkonzepten und Whitelisting im E-Mail-Marketing.

Das Thema **Datenkonzept und Zertifizierung im E-Mail-Marketing** ist in den Bereichen Daten und Technik/Sicherheit verortet. Nach einer kurzen Übersicht über unterschiedliche Datenschutz-Gutachten und Datenschutz-Siegel folgt eine Vorgehensweise für ein umfassendes Datenkonzept im E-Mail-Marketing.

1. Datenkonzept

a. Datenerfassung

Je mehr Daten – z.B. Öffnungen oder Klicks – Sie von Ihren Empfängern erheben können, desto präziser können Sie Ihre Kommunikation auf deren Präferenzen abstimmen. Die Erhebung der Daten kann anonymisiert, pseudonymisiert oder personenbezogen stattfinden. Eine Anonymisierung liegt nach § 3 Abs. 6 BDSG dann vor, wenn sich die erhobenen Daten nicht mehr bzw. nur noch mit einem unverhältnismäßig hohen Aufwand einem bestimmten Empfänger zuordnen lassen. Anonymisierte Daten sind datenschutzrechtlich nicht relevant und können von Ihnen ohne Einschränkungen genutzt werden. Bei einer Pseudonymisierung ist die Erstellung eines Clusters möglich, aber durch das Fehlen der persönlichen Ansprache wird die Entwicklung einer Vertrauensbasis beeinträchtigt.

Falls Sie personenbezogene Daten zur Bildung von Nutzungsprofilen erheben möchten, d.h. z.B. Klicks eines Empfängers mit seiner E-Mail Adresse verknüpfen, benötigen Sie eine explizite Einwilligung in eine zusätzliche Datennutzungserklärung. Diese sollte nicht an die Einwilligung zum E-Mail-Marketing gebunden sein, muss also separat erfolgen.

Die Datennutzungserklärung muss so formuliert sein, dass ein durchschnittlich verständiger Nutzer erkennen kann, dass er durch die Abgabe seiner Erklärung rechtsverbindlich der Erhebung sowie Verwendung seiner personenbezogenen Daten zustimmt. Dabei muss für den Nutzer ersichtlich sein, auf welche Daten sich die Einwilligungserklärung bezieht, zu welchen Zwecken die Daten verarbeitet und ggf. an wen die Daten weitergegeben werden sollen. Eine pauschale Einwilligung, die etwa von "allen Reaktionsdaten" spricht, ist unzulässig.

Exkurs: Privacy Admission Control dedizierte Einwilligungen verwalten.
Um die Absprungquote zu reduzieren, ist es am Beginn einer Kundenbeziehung nützlich, sich auf die wesentlichen Fragmente der Profilierung zu konzentrieren und weitere Stufen sukzessive auszubauen. Privacy Admission Control hilft im E-Mail-Marketing, zwischen acht unterschiedlichen Profilierungsebenen zu segmentieren und diese userbezogen auszubauen. Es wird differenziert zwischen der Erfassung von Standardkennzahlen, automatisierter Interessensermittlung, Bestimmung der genutzten Social Networks, Registrierung des verwendeten Endgeräts, Nutzerbezogenes Scoring, Funnel-Profiling, Ermittlung des Abruforts wie auch der Wiedererkennung anonymer Nutzer. Somit ist ein differenziertes Verwalten unterschiedlicher Datennutzungslevel möglich.

Gestaltung der Einwilligungserklärungen
Die wahrscheinlich gängigste Variante zur Einholung der Einwilligung für die Erhebung personenbezogener Daten ist eine separate Checkbox im Rahmen des Registrierungsprozesses zum E-Mail-Marketing. Folgende Varianten sind möglich:

- Vollständige Benennung einwilligungsrelevanter Passagen: Die vermutlich rechtlich sicherste Variante ist es, dem Nutzer mit der Checkbox alle wesentlichen bzw. einwilligungsrelevanten Sachverhalte konkret zu benennen.
- „Ich willige ein, dass (_FIRMA__) im Rahmen dieses E-Mail-Dienstes folgende Daten erhebt und in meinem Profil speichert:
    - konkrete Beschreibung der eingesetzten Profilierungsmethoden/die entsprechenden Passagen aus der Datennutzungserklärung)"

Eine verkürzte Benennung der einwilligungsrelevanten Passagen und Verlinkung kann vor Gericht gegebenenfalls angreifbar sein, falls das Gericht zum Schluss gelangt, dass durch die Verlinkung die konkreten einzelnen Gegenstände der Einwilligung unerwartet und überraschend für einen Verbraucher und damit unwirksam sind.

Einholung der Zustimmung im Rahmen des Double-Opt-In: Die Zustimmung zum erweiterten Tracking muss nicht zum selben Zeitpunkt erfolgen wie das Opt-In zum E-Mail-Marketing. Die Zustimmung kann ebenso zu einem späteren Zeitpunkt nachgeholt werden. Hierdurch entsteht die Möglichkeit, diese Zustimmung vom Registrierungsformular z.B. in die Double-Opt-In E-Mail zu verlagern. Die Registrierungsseite muss hierfür nicht angepasst werden. Lediglich in der Double-Opt-In E-Mail wird die typische Bestätigung des Abonnements durch die Bestätigung der erweiterten Datennutzung ersetzt. Der Zweck der Double-Opt-In E-Mail – nämlich die Verifizierung der E-Mail Adresse – wird dadurch nicht beeinträchtigt.

„Lieber Herr/Frau Name,
vielen Dank für Ihre Registrierung zum FIRMA Newsletter an Ihre E-Mail-Adresse.

Bitte bestätigen Sie zur Vervollständigung Ihrer Anmeldung unsere besonderen Regelungen zur Speicherung und Verwendung Ihrer personenbezogenen Daten sowie die Profilbildung für eine individuelle Verbesserung des E-Mail-Dienstes gemäß unserer Datenschutzerklärung.

Ja, ich bestätige die Erhebung und Verarbeitung meiner personenbezogenen Daten für den FIRMA Newsletter gemäß Datennutzungserklärung. Weitere Informationen zur Datennutzungserklärung finden Sie hier [Link]."

Es ist allerdings nicht sicher, dass die Zustimmung in dieser Form bzw. die damit verbundenen Regelungen nicht als überraschend erachtet werden. Daher sind ebenso Varianten denkbar, bei denen eine ausführlichere Erläuterung gegeben wird oder bei der ein zweiter Link nur mit Bestätigung ohne erweiterte Datennutzung angeboten wird („Wenn Sie lediglich den E-Mail-Service bestätigen möchten und der Datennutzungserklärung nicht zustimmen, klicken Sie hier"). Denkbar sind auch ein „normaler" Double-Opt-In Link und eine Zielseite (Landingpage), auf der mit einem extra Button die Zustimmung erteilt wird.

Rechtssichere Datenerfassung technisch abbilden
Die rechtssichere Erfassung von personenbezogenen Daten muss auch in der eingesetzten E-Mail-Marketing Software technisch umgesetzt werden. Die Software muss eine explizite Unterscheidung zwischen Empfängern mit verschiedenen Datennutzungszustimmungen gewährleisten. D.h., dass bei jedem Empfänger bei der Datenerfassung lediglich jene Profilierungsmethoden zur Anwendung gelangen, denen er auch zugestimmt hat. Da gesammelte Empfängerdaten im E-Mail-Marketing oftmals aus unterschiedlichen Quellen – z.B. Newsletter-Anmeldung, Gewinnspiele oder Online-Shops – mit voneinander abweichenden Datennutzungserklärungen stammen, müssen diese Datennutzungserklärungen technisch differenziert verwaltet werden. Dies gilt insbesondere im internationalen Versand, wenn Daten aus unterschiedlichen Ländern mit abweichenden Datenschutzstandards erhoben werden.

b. Datenverarbeitung

Neben der Erfassung (= Erhebung) personenbezogener Daten sind auch die weiteren Datenverarbeitungsphasen beim E-Mail-Marketing datenschutzrechtlich relevant und müssen, außerhalb der „listenmäßigen" Daten nach § 28 Abs. 3 BDSG, von der erteilten Einwilligung gedeckt sein. Der Begriff der „Verarbeitung" wird dabei sehr weit verstanden und umfasst jedes „… Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten." Über den Auffangtatbestand der „Nutzung" wird ebenso jede weitere Verwendung der Daten erfasst. Dies hat zur Folge, dass die erklärte Einwilligung nicht auf den Erhalt der Marketing-E-Mail an sich begrenzt sein darf, sondern auch nachgelagerte und beabsichtigte Datenverarbeitungsvorgänge (z.B. die Weitergabe der Daten an Tochter- oder Partnerunternehmen) einschließen muss.

Weiterhin ist zu beachten, dass wegen des Zweckbindungsgrundsatzes jede Verwendung der Daten zu einem neuen, in der Einwilligung nicht genannten, Zweck eine weitere, grundsätzlich einwilligungsbedürftige Handlung darstellt. Dem kann auch nicht durch eine beliebig weite Formulierung (z.B. „zu kommerziellen Zwecken") begegnet werden, da die Einwilligung hinreichend konkret und transparent bleiben muss. Ist der geplante Verwendungszweck in der Einwilligung nicht genannt, müssen Sie hierfür eine separate Einwilligung des Kunden einholen.

Diese Vorgaben gelten generell für die Verarbeitung und Nutzung personenbezogener Daten, also für alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Neben Name, Anschrift und E-Mail-Adresse umfasst dies auch die IP-Adresse oder Nutzungsdaten eines Websitebesuchs, wenn diese mit einer Person verknüpfbar sind.

c. Dokumentation

Beim E-Mail-Marketing kommt es nicht nur darauf an, die Daten korrekt zu erfassen und die Authentizität des Empfängers über ein Double-OptIn Verfahren zu verifizieren, sondern ebenso darauf, dass Unternehmen die rechtskonforme Erhebung der Daten im Zweifelsfall beweisen können.

Lediglich durch eine lückenlose Dokumentation des gesamten Anmelde-, aber auch des Abmeldeprozesses können Sie sich gegen etwaige Vorwürfe seitens einzelner Nutzer oder der Datenschutzbehörden verteidigen.

Das beginnt bereits beim Ausfüllen des Anmeldeformulars bzw. beim Aktivieren der Checkbox, durch die der Nutzer der Zusendung von werbenden E-Mails zustimmt. Häufig begehen Unternehmen den Fehler, nur den letzten Schritt, den Klick auf den Bestätigungslink, zu dokumentieren.

Das ist aus zwei Gründen grob fahrlässig:

1. Sie verarbeiten die Daten des Nutzers bereits, bevor dieser den Bestätigungslink anklickt. Ansonsten könnten Sie schon die Bestätigungsmail nicht versenden. Dazu benötigen Sie eine Einwilligung des Nutzers.
2. Der Klick auf den Bestätigungslink dient meist nur der Verifizierung der angegebenen E-Mail-Adresse und soll sicherstellen, dass die Anmeldung und die Einwilligung tatsächlich vom Inhaber der E-Mail-Adresse stammen. Allenfalls, wenn die E-Mail erneut den Einwilligungstext und etwa erforderliche Hinweise enthält, kann der Klick auf den Link als Einwilligung im datenschutzrechtlichen Sinne gewertet werden.

Aus diesem Grund beginnt eine aussagekräftige Dokumentation schon mit dem Anmeldeprozess. Neben den Daten, die der Nutzer eingibt, sollten Sie die Eingaben mit einem Zeitstempel versehen. Denn letztendlich müssen Sie nicht nur nachweisen, dass Sie eine Einwilligung des Nutzers haben, sondern dass Sie die Einwilligung erhalten haben, bevor Sie die erste E-Mail an ihn versenden. In Anbetracht des Vorgesagten und des Urteils des OLG München vom 27.09.2012 Az. 29 U 1682/121 gilt das insbesondere auch für die Bestätigungsmail.

Der nächste Punkt einer Dokumentation sollte der Versand der Bestätigungsmail an die angegebene E-Mail-Adresse sein. Auch hier sollte neben dem Versand, dem Inhalt der E-Mail und dem Bestätigungslink ein Zeitstempel gesetzt werden. In Bezug auf die

1 http://medien-internet-und-recht.de/volltext.php?mir_dok_id=2427

Generierung des Links sollte eine grundsätzliche Dokumentation existieren, aus der hervorgeht, wie das System sicherstellt, dass die Bestätigungsmail einen eindeutigen Link enthält. Im Streitfall muss nachvollziehbar sein, dass der Link lediglich vom Empfänger der E-Mail bestätigt werden kann/konnte.

Als vorerst letzter Schritt ist der Klick auf den Bestätigungslink inklusive eines Zeitstempels zu dokumentieren. Auch hier geht es darum, nachvollziehen zu können, dass Sie die erste werbende E-Mail erst nach Klick auf den Bestätigungslink und damit nach Verifizierung der E-Mail-Adresse versandt haben.

Der Beweiswert einer IP-Adresse ist aus zwei Gründen äußerst zweifelhaft:

1. Die IP-Adresse kann stets nur einem Internetanschluss zugeordnet werden, aber keiner konkreten Person. Identifizierbar ist allenfalls der Anschlussinhaber. Teilen sich mehrere Personen einen Internetanschluss, ist dies für den Nachweis der Einwilligung allenfalls als Indiz zu werten. Ein harter Beweis wird damit nicht gelingen.
2. Die Zuordnung dynamischer IP-Adressen zu einem konkreten Internetanschluss durch den Provider ist lediglich in einem eingeschränkten Zeitraum – aktuell 7 Tage – möglich. Nach diesem Zeitraum sind die Provider angewiesen, die für die Zuordnung notwendigen Daten zu löschen. In den seltensten Fällen werden Rechtsstreitigkeiten um die Einwilligung in diesem Zeitraum geführt.

Damit ist die Dokumentation aber noch nicht abgeschlossen. Auch die Abmeldung der Nutzer bzw. der Widerruf der Nutzer müssen dokumentiert werden. Die Dokumentation einer Abmeldung oder eines Widerruf im System muss nachvollziehbar sein.

Sollte sich ein Nutzer darauf berufen, dass Sie ihm nach der Abmeldung bzw. nach einem Widerruf weiterhin E-Mails gesendet haben, müssen Sie darlegen können, dass eingehende Abmeldungen und Widerrufe lückenlos erfasst und dokumentiert werden. Können Sie diese nachvollziehbar darlegen, liegt die Beweislast für die Abmeldung bzw. den Widerruf beim Nutzer.

Die Dokumentation selbst sollte – soweit möglich – revisionssicher sein, d.h. manuelle Eingriffe sollten weitgehend unmöglich sein. Wenn manuelle Eingriffe nicht umgangen werden können, z.B. Anmeldung für den Newsletter über ein Papierformular bei einer Veranstaltung oder Erfassung eines telefonischen Widerrufs, sollten Art und Umfang der manuellen Eingriffe ebenfalls nachvollziehbar dokumentiert werden.

d. Widerspruch

Die Tätigkeitsberichte der Datenschutzbehörden der letzten Jahre zeigen teilweise sehr deutlich, dass ein schlechtes Widerrufsmanagement im E-Mail-Marketing immer wieder Anlass für Beschwerden seitens der Nutzer und Ausgangspunkt für teilweise intensive Prüfungen seitens der Aufsichtsbehörden darstellt.

Die Gründe dafür sind vielfältig, führen jedoch alle zu datenschutzrechtlichen Beanstandungen seitens der Aufsichtsbehörden, ggf. Bußgeldern und teilweise zu

Unterlassungsansprüchen der betroffenen Nutzer. Auch wenn die bisher ausgesprochenen Bußgelder sowie die Streitwerte im Unterlassungsverfahren überschaubar sind, sollten Sie den internen Aufwand, den eine Prüfung der Aufsichtsbehörde verursacht, nicht unterschätzen. Dies gilt umso mehr, als im Rahmen der Prüfung ggf. weitere datenschutzrechtliche Baustellen zutage treten.

Die häufigsten Fehler beim Widerrufsmanagement:

- Die E-Mails enthalten keinen Abmelde-/Widerrufslink.
- Der in den E-Mails enthaltene Abmelde-/Widerrufslink funktioniert nicht bzw. nicht korrekt.
- E-Mails werden über eine sog. noreply-Adresse versandt, sodass Widerrufe über die „Antworten"-Funktion nicht eingehen.
- Abmeldungen/Widerrufe, die per Post, Fax, E-Mail oder telefonisch eingehen, werden nicht erfasst bzw. nicht oder erst verspätet berücksichtigt.
- Es wird ein veralteter Datenbestand (Backup) eingespielt, das die Widerrufe seit Erstellung des Backups nicht enthält bzw. überschreibt.
- Es existieren mehrere Datenbestände z.B. im CRM und im separaten Newslettersystem, die nicht bzw. nur unzureichend gegeneinander abgeglichen werden.
- Eine vollständige Löschung aller Daten findet nach Eingang des Widerrufs statt.

Die ersten beiden Punkte lassen sich durch ein Qualitätssicherungsmaßnahmen und Testingverfahren bei Einrichtung des Newsletter- bzw. E-Mail-Systems sehr gut ausschließen. Die Erfahrung zeigt allerdings, dass beides in regelmäßigen Abständen stichprobenartig geprüft werden sollte. Empfehlenswert ist die Aufnahme einer internen E-Mail-Adresse in den E-Mail-/Newsletterverteiler. So kann beides bei jedem Newsletter/jeder E-Mail-Kampagne getestet werden.

Aufgrund der technischen Unterschiede sollte die Anzeige der E-Mail bzw. des Newsletters in verschiedenen E-Mail-Clients geprüft werden. Dies gilt in zunehmendem Maß für E-Mail-Clients mobiler Endgeräte. Insbesondere bei der Verwendung von HTML-E-Mails muss geprüft werden, ob der Abmeldelink bzw. die Abmeldeschaltfläche auf gängigen Endgeräten/in gängigen E-Mail-Clients korrekt angezeigt werden und nutzbar sind.

Für den Versand des Newsletters/der E-Mail-Kampagnen sollte keine noreply-Adresse zum Einsatz gelangen. Die Tätigkeitsberichte der Aufsichtsbehörden zeigen, dass Nutzer immer wieder versuchen, ihre Abmeldung per E-Mail zu versenden, indem sie die Antwort-Funktion ihres E-Mail-Clients nutzen.

Ähnliches gilt für Widerrufe über das Kontaktformular der Website, eine E-Mail an eine allgemeine Adresse des Unternehmens, Abmeldungen per Brief oder telefonisch. Auch wenn die ursprüngliche Einwilligung des Nutzers elektronisch erfolgte, darf der Nutzer bei Erklärung des Widerrufs nicht auf elektronische Erklärungen beschränkt werden.

Sie müssen durch organisatorische Prozesse sicherstellen, dass auch solche Abmeldungen/Widerrufe zeitnah Berücksichtigung finden. Das lässt allerdings nicht

technisch lösen, sondern lediglich durch entsprechende organisatorische Prozesse und entsprechende Anweisung der betroffenen Mitarbeiter.

Hin und wieder wird sich eine Einspielung von Backups nicht vermeiden lassen. Um Inkonsistenzen bei den Abmeldungen/Widerrufen zu vermeiden, sollten regelmäßige Backups erstellt werden, damit bei der Einspielung eines Backups möglichst wenige Abmeldungen/Widerrufe verloren gehen bzw. überschrieben werden. Bitte achten Sie in diesem Zusammenhang auch auf die korrekte Konfiguration der Backuperstellung.

Ein ähnliches Problem entsteht, wenn die Daten der Empfänger nicht zentral, sondern an mehreren Orten gespeichert und nur unzureichend gegeneinander abgeglichen werden. Dies ist häufig der Fall, wenn die Empfängerdaten für einen regelmäßigen Newsletter in einem separaten Newslettersystem gehalten werden, während Sondernewsletter oder E-Mail-Kampagnen direkt aus dem CRM heraus versandt werden.

Ein Sonderfall, der nicht zum Widerrufsmanagement im engeren Sinne zählt, allerdings in der Praxis immer wieder zu Problemen führt, ist die vollständige Löschung von Datenbeständen nach Abmeldung bzw. Erklärung des Widerrufs. Sie dürfen die Daten nach Eingang der Abmeldung bzw. des Widerrufs zwar nicht mehr zu Werbezwecken, insbesondere nicht zum Versand werbender E-Mails nutzen, das bedeutet aber nicht, dass Sie die Daten unverzüglich vollständig löschen müssen. Schließlich müssen Sie auch weiterhin in der Lage bleiben, nachzuweisen, dass die bis zur Abmeldung bzw. bis zum Widerruf versandten Newsletter rechtmäßig versandt wurden. Das können Sie nur, wenn Sie weiterhin auf die dafür erforderlichen Daten zugreifen können. Prüfen Sie daher genau, welche Daten bei Abmeldung/Widerruf gelöscht werden können und welche Sie vielleicht zu Dokumentationszwecken weiterhin benötigen. Diese Daten sind dann – im datenschutzrechtlichen Sinne – zu sperren.

2. Datenschutz-Gutachten und Datenschutz-Siegel

Die Datenschutz-Anforderungen beim Dialogmarketing sind sehr hoch. Die Systeme müssen grundsätzlich datenschutzkonform aufgebaut sein, da für einzelne Kampagnen keine separate Prüfung vorgenommen werden kann. Für die Datenverarbeitungsprozesse im E-Mail-Marketing empfiehlt sich ein separates detailliertes Datenschutz-Gutachten oder ein Datenschutz-Siegel. Übliche Zertifizierungen sind z.B. Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001, Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein oder ePrivacyseal. Gutachten oder Siegel halten ebenso behördlichen Prüfungen stand und müssen erst nach einem längeren Zeitraum bzw. bei wesentlichen Änderungen der Technologie oder der Prozesse angepasst werden. Wichtig ist, dass solche Gutachten oder Siegel zwar Vertrauen und Akzeptanz beim Nutzen schaffen, die eigene datenschutzrechtliche Compliance-Verantwortung im Einzelfall aber nicht ersetzen.

ISO/IEC 27001

Die ISO/IEC 27001 ist eine internationale Norm zur Bewertung und Zertifizierung des Managements von Informations-Sicherheitsprozessen in Unternehmen. Neben der Informationstechnik betrachtet die ISO/IEC 27001 insbesondere die relevanten Geschäftsprozesse und beschreibt die Anforderungen, die an die Organisation und an

technische Systeme gestellt werden, sowie Aktivitäten, die geeignet sind, das auf Basis einer Risikobewertung ermittelte Sicherheitsniveau dauerhaft zu gewährleisten.

Informationen werden als Unternehmenswerte betrachtet, die es zu schützen gilt gegen die unterschiedlichsten Bedrohungen.
Informationssicherheit heißt:

- Security Policy
- Organisation der Informationssicherheit
- Management der Unternehmenswerte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebes
- Zugriffskontrolle
- Systembeschaffung, -entwicklung und -wartung
- Management von Sicherheitsvorfällen
- Erfüllung rechtlicher und organisatorischer Anforderungen

Der prozessorientierte Ansatz der ISO 27001 stellt methodisch die Kompatibilität zur DIN EN ISO 9000-Familie her.

Unabhängiges Landeszentrum für Datenschutz (ULD)
Durch ein Gütesiegel wird bescheinigt, dass die Vereinbarkeit eines Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde. Auf dieser Grundlage empfiehlt das Unabhängige Landeszentrum für Datenschutz (ULD) den Einsatz des Produktes bei den öffentlichen Stellen des Landes.

ePrivacyseal
Die ePrivacyseal ist ein Anbieter für Online-Datenschutzlösungen und vergibt nach weltweiten Zertifizierungsstandards das Datenschutz-Gütesiegel, wenn digitaler Datenschutz vorbildlich eingehalten wird. Die Zertifizierung erfolgt auf der Basis des deutschen und des EU-Datenschutzrechtes (inkl. des IAB Europe OBA Agreements). Das ePrivacyseal-Datenschutzsiegel wird vergeben, wenn ein technisches sowie ein rechtliches Gutachten zu einer guten Bewertung kommen. Dabei gelten die gleichen Kriterien für alle Unternehmen.

3. Zertifizierung und Whitelisting

Hinter dem Begriff des Whitelisting steht im Zusammenhang mit E-Mail die Absicht der E-Mail-Provider, vertrauensvolle Versender von anderen unterscheiden zu können. Eine Whitelist ist eine Positivliste: Versender, die an Whitelisting-Programmen teilnehmen, werden von Systemen bevorzugt behandelt. Die Aufnahme in eine Whitelist ist stets an Bedingungen geknüpft, die Authentizität, Seriosität und Rechtschaffenheit der Versender untermauern. Bei Nichterfüllung oder Verstößen dagegen drohen der Verweis oder gar die Aufnahme in eine Blacklist.

Generell sind drei Möglichkeiten zu differenzieren:

- Persönliches Whitelisting: Jeder E-Mail-Nutzer kann im Rahmen des E-Mail-Clients eine persönliche Whitelist anlegen und individuell pflegen. Bei WEB.DE beispielsweise können

1.000 Adressen von „Freunden und Bekannten" hinterlegt werden, die dann als erwünscht markiert und automatisch in den Posteingangsordner einsortiert werden.

- Provider-bezogenes Whitelisting: Einige Provider – wie z.B. Yahoo! – bieten eine interne Whitelist. Im Falle von Yahoo! können sich kommerzielle Massenversender kostenlos für die Aufnahme in die Whitelist anmelden und erhalten nach Prüfung bestimmter Kriterien (wie beispielsweise einer positiven Versenderreputation sowie einer mindestens 30 Tage umfassenden Sendehistorie) bestimmte Zustellprivilegien. Diese Whitelist unterliegt jedoch immer noch bestimmten Filtern, unter anderem der Filterung auf Nutzer-Ebene sowie Inhalt- und URL-Filterung. Wie schon bei der persönlichen Whitelist wird ebenso bei der Provider-bezogenen Whitelist die Einhaltung von Datenschutzrichtlinien nicht geprüft.
- Gewerbliche Whitelists: Um Massenversender, die legitime Werbemails an ihre Abonnenten versenden, zu unterstützen, in den Posteingang zu gelangen, gibt es nationale und internationale kommerzielle Anbieter von Whitelists, die sich durch Art und Umfang der zu beantragenden Zertifizierung und der gewährten Vorteile bei der E-Mail Verarbeitung (dies können z.B. Zustellvorteile sein) stark unterscheiden. Im E-Mail-gestützten E-Commerce kommt diesen Anbietern eine große Bedeutung zu, da im globalen Durchschnitt derzeit 22 Prozent aller legitimen Werbemails nicht im Posteingang ankommen, sondern als Spam klassifiziert oder sogar direkt abgeblockt werden, was ein erhebliches Geschäftsrisiko darstellt.

Da im E-Mail-Marketing die Interaktion zwischen Unternehmen und Kunde nicht wie im Webshop direkt über die Website des Unternehmens erfolgt, sondern die Kommunikation an einen E-Mail-Client eines E-Mail-Providers geschickt und von diesem erst an den Abonnenten weitergereicht wird, legen die Anbieter gewerblicher Whitelists den Fokus auf das Spannungsfeld zwischen Versender – also den Unternehmen, die Dialogkommunikation via E-Mail betreiben – und den E-Mail Providern wie WEB.DE, GMX, Gmail, Outlook.com, Yahoo! und viele andere mehr. Ziel der E-Mail Provider ist es die eigenen Nutzer bestmöglich vor z.B. Spam, Phishing oder anderweitig unerlaubter Kommunikation zu schützen. Seriöse E-Mail Versender hingegen haben ein Interesse Ihre Kommunikation von unerlaubten Versuchen der E-Mail Kommunikation zu differenzieren und als Ergebnis dieser Differenzierung eine bestmögliche Verarbeitung (bspw. Zustellung) der eigenen Kommunikation bei den E-Mail Providern zu erreichen.

Der Aufnahme in eine Whitelist geht die Zertifizierung durch den jeweiligen Anbieter voraus. Dabei werden unterschiedliche Zulassungskriterien geprüft, dabei insbesondere ob die E-Mail Kommunikation rechtlichen Rahmenbedingungen erfüllt, z.B. durch eine Prüfung des Opt-In. Einen Überblick über die drei wichtigsten Zertifizierer für Deutschland und Europa finden Sie im Anschluss:

- Die **Certified Senders Alliance** (CSA). Das Gemeinschaftsprojekt von eco und dem DDV bietet zertifizierten Versendern ein Whitelisting bei einigen großen E-Mail-Providern, darunter z. B. Yahoo! und GMX. Versender müssen für die Aufnahme in die Whitelist bestimmten Kriterien entsprechen, die im Dokument „Aufnahmekriterien für Massenversender" detailliert dargestellt werden. Darunter fällt z.B. das Vorliegen einer Einwilligung im Sinne von § 7 Abs. 2 Nr. 3 UWG und der Einsatz von Domain Key Identified Mail (zwingende Voraussetzungen) bzw. das oben erwähnte Double Opt-In Verfahren (als Empfehlung), sowie der Hinweis, dass der Versender dafür verantwortlich ist, „dass der

Versand rechtmäßig erfolgt und insbesondere die Inhalte der versandten E-Mails nicht gesetzlichen Verboten und Geboten zuwiderlaufen". Beschwerden gegen Massenversender werden durch die eco Hotline gesammelt und bearbeitet.

- **trustedDialog**. Bei trustedDialog handelt es sich um einen von WEB.DE, GMX, Deutsche Telekom und freenet definierten Qualitätsstandard für die E-Mail Kommunikation, der die im deutschsprachigen Raum am weitest verbreiteten E-Mail Provider umfasst. trustedDialog prüft teilnehmende Unternehmen in einem mehrstufigen Prozess. Dabei werden neben oben beschriebenen CSA-Regularien auch andere Verpflichtungen seitens der versendenden Unternehmen eingehalten. trustedDialog fordert z.B. die „strikte Einhaltung der Vorschriften des Telemediengesetzes" (TMG) sowie „alle weiteren gesetzlichen Bestimmungen, welche durch die trustedDialog Nutzung angesprochen sind". Basis ist dabei eine langfristige Vertragsbeziehung zwischen dem teilnehmenden Unternehmen und dem Anbieter trustedDialog. Es findet ein kontinuierliches IP und insbesondere Domain Monitoring des teilnehmenden Unternehmens statt. Diese Kombination aus direkt zuordenbarer Verantwortung und vertraglicher Absicherung ermöglicht es den teilnehmenden Unternehmen von verschiedenen Vorteilen im Bereich der E-Mail Verarbeitung zu profitieren die neben der Zustellung in die Inbox auch eine aufmerksamkeitsstarke Darstellung der E-Mail mit dem Unternehmens-Logo umfasst und zudem die Möglichkeit aktive Elemente wie z.B. Videodirekt in der E-Mail abzuspielen. . Als selbstbetriebenes Authentifizierungsprogramm der genannten E-Mail Provider stehen bei diesem Ansatz sehr stark die Nutzerakzeptanz, -vertrauen und -sicherheit im Vordergrund. Die über trustedDialog verarbeitete Kommunikation und der damit verbundene Qualitätsanspruch werden daher auf allen Endgeräten direkt mit einem E-Mail Siegel visualisiert und zeigen den Nutzern eindeutig, dass es sich um geprüfte, authentifizierte Kommunikation frei von Gefahren wie Spam & Phishing handelt.
- **Return Path**. Als Anbieter von E-Mail Intelligence Lösungen legt Return Path seinen Fokus darauf, dass lediglich erwünschte E-Mails den Posteingang erreichen. Deshalb verfügt Return Path in seinem Lösungsportfolio neben dem Whitelisting-Angebot, der Return Path Zertifizierung, ebenso über Anti-Phishing-Lösungen und ist in der Lage, über ein Panel tatsächlicher E-Mail-Abonnenten deren Interaktion mit Werbemails darzustellen und im Unternehmens- sowie Branchenvergleich zu bewerten. Das Whitelisting-Angebot ist stark international fokussiert und beinhaltet neben zwei der drei weltweit größten Mailbox-Provider (Yahoo! und Microsoft mit Outlook.com, ehemals Hotmail) auch viele regionale Provider, sodass global über zwei Milliarden Posteingänge sicher zu erreichen sind. Die Aufnahme erfolgt nach Prüfung vielfältiger Kriterien, u.a. nach einem Audit der Opt-In-Prozesse und einer Prüfung von Datenschutzrichtlinien, und ist zu einem großen Teil technologiebasiert. So wird die Reputation des Versenders anhand verschiedenster Reputationskriterien und entsprechender Kennzahlen vor und während der Zertifizierung laufend geprüft. Bei Überschreiten der Grenzwerte werden die problematischen IPs selektiv, sprich für den Provider, bei dem das Problem auftrat, von der Whitelist suspendiert, nach erneutem Bestehen aller Kennwerte aber automatisch reaktiviert. Return Path zertifizierte Versender erhalten Zugang zu einer Softwarelösung, in der sie stets aktuell die wichtigsten Kennzahlen einsehen können. Überdies werden tägliche Performance-Reports geliefert.

4. Summary

E-Mail-Marketing bedeutet das ideale Instrument, um nicht nur kurzfristige Kaufimpulse zu setzen, sondern eine langfristige, nachhaltige Kundenbeziehung mittels individualisierter Kommunikation aufzubauen. Für die individualisierte Ansprache potenzieller Interessenten oder Kunden müssen personenbezogene Daten erhoben werden, die einem besonderen Schutz unterliegen. Die personenbezogene Erhebung darf lediglich mit expliziter Zustimmung des Empfängers erfolgen. Es ist zwingend erforderlich, zu Beginn ein umfassendes Datenkonzept zu erarbeiten, um auf Grundlage dieses Konzeptes die Erfassung und Verarbeitung sensibler Daten datenschutzkonform umsetzen zu können. Das Datenkonzept sollte folgende Punkte enthalten:

- Umfang der beabsichtigten Datenerhebung
- Wege der Dokumentation von Anmeldung bis zur Abmeldung eines Empfängers
- Umfang der benötigten Zustimmung
- Formale und technische Sicherstellung der Datenschutzanforderungen

Eine Zertifizierung zeigt, dass es sich um einen professionellen Anbieter handelt, der es versteht, Kundendaten zu schützen. Mit Whitelisting wird sichergestellt, dass E-Mails (z.B. Opt-In-Mails) korrekt zugestellt und nicht fälschlicherweise als SPAM klassifiziert werden.

Hinweis: Bei diesem Dokument handelt es sich um eine Zusammenfassung wesentlicher Eckpunkte. Eine juristische Prüfung des einzelnen Prozesses ist unabdingbar, daher lassen Sie durch einen Juristen oder Ihren Datenschutzbeauftragen prüfen, ob Ihre Prozesse den rechtlichen Anforderungen entsprechen.

Autoren

Prof. Dr. Christoph Bauer
Geschäftsführender Gesellschafter, ePrivacyconsult GmbH

Christoph Becker
Head of trustedDialog Products, United Internet Dialog GmbH, Stv. Vorsitzender Initiative E-Mail im BVDW

Bernhard Kelz
Consultant, queo GmbH

Stefan Mies
Senior Marketing Manager, artegic AG, Vorsitzender Initiative E-Mail im BVDW

Dr. Fabian Niemann
Partner, Bird & Bird LLP,

Jan Niggemann
Regional Director - Central Europe, Return Path Deutschland GmbH, Leiter des Lab E-Mail Unternehmensbefragung im BVDW

Dirk Thum
Director Sales & Marketing, Selligent GmbH