Kann man Sperrlisten im E-Mail-Marketing DSGVO-konform nutzen? *

I. Problemstellung

Es ist gängige Praxis bei E-Mail Service Providern (ESPs), dass mandantenspezifische oder gar globale Sperrlisten geführt werden, um zu verhindern, dass E-Mail-Adressen wieder ins System importiert werden können, die unter keinen Umständen erneut angeschrieben werden sollen. Beispielsweise weil ein Empfänger sich in der Vergangenheit beschwert hatte und explizit wünscht, keine E-Mails mehr von diesem Versender zu erhalten.
Ein versehentlicher Reimport der betroffenen Adresse würde nicht nur den Empfänger verärgern, sondern auch die Reputation des Versenders schädigen.
Das Speichern trotz eines Widerspruchs oder Löschersuchens durch einen Empfänger könnte den datenschutzrechtlichen Bestimmungen widersprechen. Wird die betroffene E-Mail-Adresse allerdings von einer Sperrliste entfernt besteht die Gefahr, dass der Empfänger wieder angeschrieben werden könnte.

II. Mögliche technische Vorgehensweisen bei Erstellung einer Sperrliste

Erster, simpler Lösungsansatz (Variante 1)

Anstelle der E-Mail-Adresse im Klartext wird lediglich ein sogenannter Hash-Wert auf der Sperrliste gespeichert. Wird ein entsprechender Hash-Algorithmus für die Generierung des Hash-Wertes eingesetzt, ist eine Rückführung vom Hash-Wert zur ursprünglichen E-Mail-Adresse nicht ohne Weiteres möglich. Wird nun versucht Adressen ins System zu importieren, muss zu jeder zu importierenden Adresse nach demselben Algorithmus ein Hash-Wert erzeugt werden. Dieser Wert wird mit den Werten der Sperrliste abgeglichen. Erhält man eine Übereinstimmung ist klar, dass die zugehörige Adresse gesperrt ist und nicht importiert werden darf.

Problem der Variante 1

Variante 1 hat zwei entscheidende Schwächen. Die erste besteht darin, dass Hash-Algorithmen „altern". Sprich ein Hash-Algorithmus der jetzt als sicher gilt, wird in Zukunft unter Umständen durch technische Entwicklungen nicht mehr unumkehrbar sein, und somit können aus bestehenden Hash-Werten die ursprünglichen E-Mail-Adressen rekonstruiert werden. Beispielsweise gilt der bekannte Hash-Algorithmus Message-Digest Algorithm 5 (MD5), der 1991 entwickelt wurde, heute als nicht mehr sicher.

Darüber hinaus besteht das Problem so genannter Rainbow Tables. Prinzipbedingt muss ein Hash-Algorithmus bei gleicher Eingabe auch das gleiche Ergebnis liefern. Das lässt sich potentiell nutzen um mit überschaubarem Zeit- und Ressourcenaufwand, vereinfacht gesagt, eine sehr große Tabelle anzulegen in der einmalig sämtliche möglichen Eingabewerte und die zugehörigen Hash-Werte errechnet und abgelegt werden. In dieser Tabelle können dann Hash-Werte nachgeschlagen und damit die ursprüngliche E-Mail-Adresse rekonstruiert werden.

Verbesserung aus technischer Sicht (Variante 2)

Die Probleme dieses ersten Ansatzes können jedoch abgefangen werden. Die „Alterung" der Algorithmen ist nicht zu verhindern. Allerdings kann man einen Hash-Wert, der mit einem Algorithmus erstellt wurde der als nicht mehr sicher zu betrachten ist, mit einem neuen, modernen und sicheren Algorithmus erneut „hashen". Der alte Hash-Wert wird dabei zum Eingabewert für den neuen Algorithmus. Nachdem dieser Schritt vollzogen wurde, kann der alte Hash-Wert gelöscht werden. Allerdings muss bei diesem Verfahren das „Rezept", mit dem man den letztlichen Hash-Wert auf der Sperrliste erhalten hat, ebenfalls dokumentiert werden, damit eine Gegenprüfung von Adressen gegen die Sperrliste auch weiterhin möglich ist.

Das Problem mit Rainbow Tables kann durch einen „salt" umgangen werden. Ein salt ist ein idealerweise zufälliger Wert, der dem eigentlichen Wert – also z.B. der E-Mail-Adresse – angehängt wird bevor man den Hash berechnet. Der salt muss für seine Wirksamkeit nicht geheim gehalten werden und kann zusammen mit dem Hash-Wert und dem „Rezept" in der Sperrliste gespeichert werden. Auch bei dieser Variante 2 wäre es theoretisch möglich, zu jedem potentiell existierenden salt eine eigene Rainbow Table zu erstellen. Also müsste man statt einer einzigen sehr großen Tabelle nun extrem viele solcher Tabellen erstellen. Allerdings wäre hierzu ein solch massiver Ressourcen- und Zeitaufwand nötig, dass es nicht mehr ansatzweise praktikabel ist.

III. Rechtliche Bewertung der beiden vorgestellten Ansätze

Im Rahmen der rechtlichen Prüfung soll im Folgenden bewertet werden, inwiefern die beiden vorgestellten technischen Vorgehensweisen mit der EU-DSGVO vereinbar sind. Hierfür muss zunächst geklärt werden, inwiefern Sperrlisten personenbezogene Daten enthalten, da die DSGVO nur in diesem Falle anwendbar ist.

Personenbezogene Daten

Der Anwendungsbereich der DSGVO ist dann eröffnet, wenn personenbezogene Daten verarbeitet werden. Der Begriff der personenbezogenen Daten wird in Art. 4 Abs. 1 Nr. 1 DSGVO[1] definiert. Danach sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Betroffenen sind identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden können, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen sind. In der Praxis fallen darunter also sämtliche Daten, die auf jedwede Weise einer Person zugeordnet werden oder zugeordnet werden können.

E-Mail-Adressen werden zu den personenbezogenen Daten gezählt.[2] Fraglich ist, ob bei E-Mail-Adressen durch das Einsetzen von Hashwerten die Regelungen der DSGVO anwendbar sind. Für die Bejahung der Anwendbarkeit müsste es sich bei Hashwerten ebenfalls um personenbezogene Daten handeln. Entscheidend ist an dieser Stelle, ob es sich bei dem Einsatz von Hash-Algorithmen um eine Pseudonymisierung oder Anonymisierung handelt.

Abgrenzung Pseudonymisierung und Anonymisierung

Im Rahmen einer Pseudonymisierung genügt jede Veränderung eines Datensatzes, die die Zuordnung zu einer natürlichen Person erschwert, wenn über zusätzliche Informationen und Zusatzwissen die Zuordnung wiederhergestellt werden kann. Unerheblich hierbei ist, ob das Zusatzwissen tatsächlich in Anspruch genommen wird. Nur für den Fall, dass das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, würde man den Anforderungen einer Anonymisierung genügen[3] und nicht mehr von einer reinen Pseudonymisierung ausgehen. Einer Pseudonymisierung unterzogene personenbezogene Daten werden als Informationen über eine identifizierbare natürliche Person betrachtet.

Bei der Anonymisierung erfolgt eine über die Pseudonymisierung hinausgehende Datenminimierung, so dass ein Personenbezug überhaupt nicht mehr hergestellt werden

[1] Nicht näher bezeichnete Artikel sind solche der DSGVO
[2] https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php
[3] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 4 Rdnr. 76

kann oder nur mit einem unverhältnismäßigen Aufwand (s.o.). Die Verarbeitung wirksam anonymisierter Datensätze ist datenschutzrechtlich nicht eingeschränkt.

Personenbezogene Daten in Variante 1

Durch den Einsatz von Hash Algorithmen gemäß Variante 1, wie oben beschrieben, wird die Zuordnung zu einer bestimmten Person zwar etwas erschwert, ist aber ohne viel Aufwand möglich. Bei dieser Variante handelt es sich um eine Pseudonymisierung von personenbezogenen Daten, die den datenschutzrechtlichen Vorschriften unterliegt.

Personenbezogene Daten in Variante 2

Vorliegend dürfte die Zuordnung zu der betroffenen E-Mail-Adresse nur mit sehr erheblichem Zeit- und Arbeitsaufwand und mit üblicherweise zur Verfügung stehenden Mitteln nicht möglich sein. Selbst für staatliche Institutionen, die über weitergehende Möglichkeiten verfügen, wäre das Ermitteln der hinter dem Hashwert stehenden E-Mail-Adresse, wenn überhaupt, nur unter erschwerten Bedingungen möglich. Das Vorgehen dürfte nicht mehr unter dem datenschutzrechtlichen Begriff der Pseudonymisierung definiert werden. Vielmehr ist von einer Anonymisierung auszugehen.

Zwischenergebnis

Durch Einsetzen von Variante 1 besteht die Gefahr, dass die Zuordnung zu der betroffenen Person weiterhin ohne erheblichen Aufwand möglich ist, mit der Folge, dass es sich um eine Pseudonymisierung handelt. Es müssen mithin die datenschutzrechtlichen Vorschriften beachtet werden. Die DSGVO ist somit anwendbar.

Anders ist die Rechtslage bei der Verwendung der Hash Methode nach Variante 2 zu bewerten. Aufgrund des unzumutbaren Aufwands, der bei einer Zuordnung der Daten zu der betroffenen Person entstehen würde, ist von einer Anonymisierung auszugehen. Somit sind keine personenbezogenen Daten in Variante 2 enthalten. Der Einsatz ist daher aus datenschutzrechtlicher Sicht grundsätzlich unbedenklich.

Vereinbarkeit der Variante 1 mit der DSGVO

Haben Unternehmen nur die Möglichkeit die Variante 1 einzusetzen, stellt sich die Frage, ob dieses Vorgehen überhaupt datenschutzrechtlich möglich ist. Gemäß Artikel 6 Abs. 1 DSGVO ist die Verarbeitung von personenbezogenen Daten nur dann zulässig, wenn entweder eine Einwilligung des Betroffenen oder ein anderer Erlaubnistatbestand vorliegt. In Betracht kommen im Wesentlichen das Vorliegen einer Einwilligung gemäß Artikel 6 Abs. 1 lit. a und der Erlaubnistatbestand nach Artikel 6 Abs.1 lit. f, der die Verarbeitung bei Vorliegen eines berechtigten Interesses des Verantwortlichen erlaubt, wenn nicht schützenswerte Interessen des Betroffenen überwiegen.

a) Einwilligung nach Art. 6 Abs.1 lit. a

Die Verarbeitung personenbezogener Daten einer betroffenen Person für einen oder mehrere Zwecke ist nach Art. 6 Abs. 1 Nr. lit. a rechtmäßig, wenn sie hierzu ihre Einwilligung abgegeben haben. Eine Einwilligung muss für einen bestimmten Fall in informierter Weise freiwillig erteilt werden und die in Art. 7 benannten allgemeinen Anforderungen erfüllen.[4]

Unternehmen, die den Einsatz von Variante 1 rechtmäßig implementieren möchten, müssten folglich vorher eine formell rechtmäßige Einwilligung des Betroffenen einholen. Die Verantwortlichen müssten mithin an jede Person gesondert herantreten und eine Einwilligung zur Verarbeitung der E-Mail-Adresse zwecks Erstellung einer Sperrliste erfragen. Weiterhin müsste jede Einwilligungserklärung zwecks Beweissicherung dokumentiert werden. Auch wenn die Einwilligung das rechtssicherste Mittel darstellen würde, so dürfte die Einholung für die meisten Unternehmen nicht sehr praktikabel sein, insbesondere dann nicht, wenn die Einwilligung im Nachgang von jeder einzelnen betroffenen Person eingeholt werden soll.

Ein denkbarerer Ansatz könnte sein, die Einwilligung zur Verwendung der E-Mail-Adresse für die Erstellung einer Sperrliste zeitgleich mit der Einholung der Einwilligung für die Versendung von Werbe-E-Mails einzuholen. In diesem Fall müssen zwingend die formellen Anforderungen von Art. 7 DSGVO beachtet und zwei separate Einwilligungserklärungen formuliert werden. Darüber hinaus kann der Betroffene seine Einwilligung zur Verwendung seiner Daten auch zum Zwecke der Erstellung einer Sperrliste widerrufen, Art. 7 Abs. 3.

[4] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 6 Rdnr. 16

b) berechtigtes Interesse nach Art. 6 Abs. 1 lit. f

Die Regelung in Art. 6 Abs. 1 lit. f lässt die Verarbeitung personenbezogener Daten zu, wenn dies zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritten erforderlich ist. Die Zulässigkeit einer Verarbeitung auf Grundlage dieses Erlaubnistatbestandes steht unter dem Vorbehalt, dass es keine überwiegenden Interessen oder Grundrechte und Grundfreiheiten betroffener Personen gibt, die den Schutz der personenbezogenen Daten erfordern. Die notwendige Interessenabwägung obliegt dem Verantwortlichen.[5] Die Interessen des Betroffenen betreffen den Schutz der eigenen personenbezogenen Daten.

Hat der Betroffene der Verwendung seiner personenbezogenen Daten zur Verwendung der werblichen Ansprache per E-Mail widersprochen, so könnte man trotzdem eine Rechtfertigung der Verarbeitung dieser Daten in einer Sperrliste bejahen. Der Verantwortliche möchte durch Anlegen einer Sperrliste sicherstellen, dass E-Mail-Adressen, für deren Verwendung ein Widerruf der Einwilligung zur werblichen Ansprache erfolgt ist, nicht erneut zu diesem Zweck verwendet werden kann. Die erneute bewusste oder versehentliche Verwendung der E-Mail-Adresse des Betroffenen zur werblichen Ansprache soll somit verhindert werden. Durch eine Pseudonymisierung sind die Daten auch grundsätzlich vor einem unberechtigten Zugriff Dritter geschützt und somit sinkt die Gefahr einer Zuordnung.

Da durch diese Vorgehensweise die Interessen des Betroffenen unterstützt werden, ist das legitime Interesse des Verantwortlichen mit großer Wahrscheinlichkeit zu bejahen. Es stellt sich die Frage, wie sich die Rechtslage bei einem Löschersuchen des Betroffenen gestaltet.

Gemäß Artikel 17 DSGVO kann die betroffene Person die Löschung der sie betreffenden personenbezogenen Daten verlangen und der Verantwortliche muss diese Daten unverzüglich löschen, sofern einer der Gründe in Art. 17 Abs. 1 lit. a-f einschlägig ist und kein Ausnahmetatbestand gemäß Art. 17 Abs. 3 vorliegt. Interessant könnten Art.17 Abs. 1 li. b und c sein: Demnach wäre die E-Mail-Adresse des Betroffenen zu löschen, wenn ein Widerruf bzw. Widerspruch vorliegt und keine anderweitige Rechtsgrundlage zur Verarbeitung vorliegt.

[5] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 6 Rdnr. 90 ff.

Als anderweitige Rechtsgrundlage kommt wiederum das berechtigte Interesse des Verantwortlichen gemäß Art. 6 Abs. 1 lit. f in Betracht. Insoweit kann auf die Argumentation des berechtigten Interesses verwiesen werden.

IV. Fazit und Empfehlungen:

Der Einsatz der Variante 1 ist grundsätzlich problematisch. Da die Zuordnung zu der hinter der E-Mail-Adresse stehenden Person ohne unverhältnismäßigen Aufwand möglich ist, müssen datenschutzrechtliche Anforderungen beachtet werden. Eine legitime Verarbeitung ist unter Abwägung der jeweiligen Interessen zwar denkbar, bietet aber keine hundertprozentige Rechtssicherheit. Größere Rechtssicherheit bietet die Einwilligung: Die Einholung einer vorherigen Einwilligung müsste jedoch zwingend den strengen, formalen Anforderungen der DSGVO genügen.

Folglich ist die Variante 2 daher vorzugswürdig. Da eine Zuordnung der E-Mail-Adresse zu der betroffenen Person nur mit unverhältnismäßigen Mitteln möglich wäre, ist nach vorliegender Betrachtung von einer Anonymisierung auszugehen, die nicht vom datenschutzrechtlichen Anwendungsbereich umfasst ist.

Stand: November 2018

**Rechtlicher Hinweis: Dieser Artikel erhebt keinen Anspruch auf Rechtssicherheit und Vollständigkeit. Er soll auf die möglichen Probleme hinweisen.*

Autoren: Alexander Zeh, Engineering Manager
und Rosa Hafezi, Legal Counsel
Certified Senders Alliance