Kriterien

für die Teilnahme von E-Mail-Versendern an der
Certified Senders Alliance (CSA) – CSA Kriterien

1 Präambel

Das vorliegende Dokument beschreibt die von eco – Verband der Internetwirtschaft e. V. (eco) und dem Deutschen Dialogmarketing Verband e. V. (DDV) gemeinsam definierten Kriterien für die Teilnahme von E-Mail-Versendern an der CSA.

Die Erfüllung der aufgestellten Kriterien gewährleistet nicht die Zustellung von E-Mails an die adressierten Nutzer, da von diesen vorgenommene Filtereinstellungen oder Maßnahmen von Internet Service Providern (ISP) zur Aufrechterhaltung der Netzwerksicherheit und Dienstestabilität eine Zustellung verhindern können.

2 Zwingende Kriterien

Benennung von IP-Adressen

2.1 Grundsätzlich sind alle vom zertifizierten Versender für den E-Mail-Versand genutzten IP-Adressen auf der Whitelist zu führen. Die Nutzung von nicht auf der Whitelist geführten IP-Adressen ist ausschließlich für die ersten drei Versandaktionen von Neukunden zulässig, wenn seit dem Zeitpunkt der ersten Versandaktion nicht mehr als zwei Monate vergangen sind. Versandaktion bedeutet das zeitlich zusammenhängende Aussenden einer im Wesentlichen inhaltsgleichen E-Mail an einen im Voraus bestimmten Empfängerkreis. Unabhängig davon, ob die IP-Adressen auf die Whitelist gesetzt werden sollen oder nicht, hat der Versender die Namen und IP-Adressen aller verwendeten E-Mail-Ausgangsserver gegenüber der CSA zu benennen. IP-Adressen, die nicht auf der Whitelist geführt werden sollen, muss der Versender explizit benennen.

Permission

2.2 Einwilligung

Der Versand von E-Mails (Werbe-E-Mails/Newsletter) erfolgt grundsätzlich nur an Adressaten, die hierzu ihre vorherige Einwilligung[1] erteilt haben (Opt-in). Diese Einwilligung muss insbesondere folgende Voraussetzungen erfüllen:

a. Die Einwilligung muss aktiv und gesondert erfolgen. Der Adressat muss entweder ein Kästchen anklicken/ankreuzen oder eine vergleichbar eindeutige Erklärung seiner Zustimmung abgeben. Diese Erklärung darf sich nur auf Werbung beziehen und nicht Bestandteil anderer Erklärungen (zum Beispiel Einwilligung in allgemeine Geschäftsbedingungen oder allgemeine Datenschutzbestimmungen) sein.

b. Die Einwilligung muss für den konkreten Fall und in informierter Weise abgegeben worden sein. Der Begünstigte der Einwilligung muss konkret benannt sein. Auch die Branchen und Bereiche, für die geworben werden soll, müssen klar und verständlich angegeben sein.

c. Die CSA weist darauf hin, dass eine Einwilligung Minderjähriger nur wirksam ist, wenn:
- das 16. Lebensjahr vollendet ist oder
- die Erziehungsberechtigten eingewilligt haben.2

d. Beim Einholen der Einwilligung ist klar und deutlich darauf hinzuweisen, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Der Hinweis muss Informationen dazu enthalten, wie und gegenüber wem der Widerruf erfolgen kann. Die Möglichkeit des Widerrufs darf nicht komplizierter als das Erteilen der Einwilligung sein. Der erfolgte Widerruf muss nach spätestens fünf Werktagen umgesetzt sein.

2.3 Ausnahmsweise können auch ohne ausdrückliches Opt-in (siehe Ziffer 2.2) unter folgenden Voraussetzungen[3] E-Mails an Kunden versendet werden:

a. bestehende Kundenbeziehung (Vorliegen eines entgeltlichen Austauschvertrags),

b. Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen,

[1] Gemeint ist eine Einwilligung entsprechend den Vorgaben der DSGVO und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 und den nationalen Implementierungen.
[2] Diese Regelung beruht auf der DSGVO. Aktuell kann noch keine Umsetzungsempfehlung gegeben werden. Daher wird ein Verstoß gegen diese Voraussetzung bis zur Klärung mit den Datenschutzbehörden, mindestens jedoch bis zum 01.07.2020, im Beschwerdefall nicht zu einem Hinweis führen.
[3] Die Voraussetzungen entsprechen den Vorgaben von Art. 13 Abs. 2 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 und den nationalen Implementierungen.

c. Hinweis auf die jederzeitige Widerspruchsmöglichkeit (bei Erhebung und jeder Verwendung der E-Mail-Adresse), ohne dass hierfür andere als Übermittlungskosten nach den Basistarifen entstehen, und

d. kein Widerspruch erfolgt.

2.4 Beim Verwenden von E-Mail-Adressen, die der Versender beziehungsweise seine Kunden von Dritten erworben haben, gilt:

a. Der Versender beziehungsweise sein Kunde muss sich vor der Vornahme von Werbehandlungen vergewissern, dass eine Einwilligung (siehe Ziffer 2.2) vorliegt. Diese Einwilligung muss sich explizit auch auf den Versender beziehungsweise seinen Kunden beziehen.

b. Bei der Datenerhebung muss für den Nutzer die Kenntnisnahme der Liste der begünstigten Unternehmen leicht und eindeutig möglich gewesen sein.

c. Die Anzahl der Unternehmen beziehungsweise Personen, für die die Adressdaten erhoben worden sind, war auf ein Maß reduziert, das das Weiterleiten der Nutzerdaten an einen unverhältnismäßig großen Kreis Dritter ausschließt. Die Anzahl muss dem Nutzer erlauben, die Tragweite und den Umfang seiner Einwilligung einfach zu erfassen sowie den rechtmäßigen Umgang mit seinen Daten einfach zu kontrollieren.

Klarstellend sei darauf hingewiesen, dass die Unternehmen, für die die Adressdaten generiert werden, diese Adressdaten nicht an Dritte weitergeben dürfen, ohne dass vom Nutzer dafür gesondert eine weitere Einwilligung eingeholt wurde.

Design of the Email

2.5 Der Auftraggeber, das heißt der Vertragspartner des zertifizierten Versenders, muss klar erkennbar sein. In jeder versendeten geschäftsmäßigen E-Mail muss ein leicht erkennbares Impressum[4] als Volltext enthalten sein. Das Impressum muss die nachfolgenden Angaben enthalten:

a. den Namen und die Anschrift, unter der der Auftraggeber niedergelassen ist, bei juristischen Personen zusätzlich die Rechtsform, das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind und die entsprechende Registernummer;

b. Kontaktinformationen, mindestens jedoch eine gültige Telefonnummer oder ein elektronisches Kontaktformular, sowie eine E-Mail-Adresse und

[4] Impressum im Sinne von Artikel 5 Abs. 1 der EU E-Commerce Directive 2000/31/EC und der nationalen Implementierungen (zum Beispiel in Deutschland § 5 Abs. 1 Telemediengesetz (TMG))

c. eine Umsatzsteueridentifikationsnummer oder eine Wirtschaftsidentifikationsnummer, sofern vorhanden.

Weitergehende Informationspflichten nach nationalen Gesetzen bleiben unberührt.

2.6 In jeder E-Mail ist darauf hinzuweisen, dass die Zusendung weiterer E-Mails abbestellt werden kann (Opt-out). Das Abbestellen von E-Mails muss grundsätzlich durch den Empfänger ohne Kenntnis von Zugangsdaten (beispielsweise Login und Passwort) möglich sein. Ausnahmen können im Einzelfall durch die eco Beschwerdestelle zugelassen werden, wenn eine abweichende Handhabung aufgrund von Besonderheiten des angebotenen Dienstes erforderlich ist; vergleiche Ziffer 2.18 bezüglich „List-Help".

2.7 In der Kopf- und Betreffzeile der E-Mail darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

Technische Konfiguration

2.8 Die Server des Versenders müssen angemessen technisch abgesichert sein (zum Beispiel mit einer Firewall, kein Open Relay, kein Public Proxy, keine Backscatter, stetig überwachte Server etc.).

2.9 Jede versendete E-Mail (Aufbau und Komposition) sowie der E-Mail-Versand (Envelope-Kommunikation im SMTP-Dialog) müssen konform zu den Request for Comments (RFC) der IETF sein.

Maßgebend sind die jeweils aktuellen RFC, unter anderem zu SMTP. Zum Zeitpunkt der Erstellung dieses Dokuments sind das unter anderem RFC 2045–2048, 2142, 5321, 5322 und 5335.

2.10 Die IP-Adresse des versendenden Mail-Servers beziehungsweise die IP-Adresse, die eine E-Mail an den ISP übergibt, muss Reverse via PTR auflösbar sein. Der Eintrag muss in der Form eines Fully Qualified Domain Name (FQDN) sein. Der verwendete FQDN muss als A-Record eindeutig auf die IP-Adresse des Mail Transfer Agent (MTA) zeigen. Der im DNS eingetragene und verwendete FQDN muss im SMTP-Dialog (Envelope-Kommunikation) beim HELO/EHLO-Kommando angegeben werden. Der Hostname darf nicht die IP-Adresse des Servers enthalten (zum Beispiel server-80-12-54-125.example.org).

2.11 Die Whois-Angaben der IP-Adresse oder des zugehörigen FQDN müssen eindeutig auf den zertifizierten Versender verweisen. Darüber hinaus müssen IP-Adresse und FQDN erreichbare Kontakt-E-Mail-Adressen sowie einfach auffindbare, allgemeine Abuse-E-Mail-Adressen im Whois enthalten (siehe unter anderem RFC 2142, RFC 3013 Section 2.5 und aktuelle Richtlinien/Best Practices der Regional Internet Registries (RIR) und anderer Registries).

2.12 Der Versender muss die alleinige Kontrolle über die versendenden Mail-Server haben. Sofern die verwendeten Mail-Server „gemietet" sind (zum Beispiel über Hoster oder ISP), muss sichergestellt sein, dass es sich hierbei um dedizierte Server beziehungsweise IPs handelt.

2.13 Die vom Versender benannten E-Mail-Ausgangsserver dürfen nur für den Massenversand beziehungsweise automatisierten Versand verwendet werden. Idealerweise muss es zum Beispiel möglich sein, spezifische Kampagnen beziehungsweise Aussendungen bestimmten dedizierten Systemen zuzuordnen.

2.14 Für die in der SMTP-Kommunikation zwischen E-Mail-Servern angegebene MAIL-FROM-Adresse ist ein SPF-From Record einzutragen, der es SPF-Systemen auf der Empfängerseite erlaubt, einen SPF-Test durchzuführen (hierzu sind vom Versender gegebenenfalls auch SRS-Verfahren einzusetzen). Der SPF-Record muss mit „-all" oder „~all" enden.

2.15 Es muss ein so genannter SPF-HELO-Eintrag für den FQDN des sendenden E-Mail-Servers vorhanden sein, der mit „-all" enden sollte, äquivalent zu den eingetragenen Informationen aus Ziffer 2.11.

2.16 Bezüglich der in der Envelope-Kommunikation zwischen E-Mail-Servern angegebenen MAIL-FROM-Adresse müssen für deren Domainnamen-Teil ein unter Umständen zusätzlicher und eventuell mit niedrigster Priorität versehener MX-Record und ein A-Record existieren, die wiederum beide auf den sendenden E-Mail-Server zeigen.

2.17 Das Verfahren DomainKeys Identified Mail (DKIM)[5] ist spätestens ab erfolgreicher Zertifizierung durch die CSA für alle zu zertifizierenden Server/IP-Adressen einzusetzen. Die in dem DKIM-„d="-Tag verwendete Domain muss via Whois-Eintrag entweder auf den zertifizierten Versender oder den betroffenen Kunden des zertifizierten Versenders zeigen. Die signierten Header müssen mindestens „From", „X-CSA-Complaints", „List-Unsubscribe" und „List-Unsubscribe-Post"[6] umfassen.

2.18 In der E-Mail muss ein „List-Unsubscribe"-Header (siehe RFC 2369)[7] mit „POST HTTPS"-Link inklusive „One-Click-Unsubscribe"-Funktionalität (RFC 8058)[8] eingefügt werden, wobei die ausschließliche Verwendung eines Mailto-Links im Rahmen der CSA nicht zulässig ist. Die angegebenen Links müssen eine direkte One-Click-Abmeldung mindestens auf Listenebene bewirken. Der Versender kann dem Nutzer eine Bestätigungs-E-Mail für eine erfolgte Abmeldung übersenden.

Ausnahmen von dieser Verpflichtung können geltend gemacht werden, wenn es aus Gründen der Ausgestaltung des Dienstes und der damit einhergehenden Zusendung automatisierter E-Mails nicht erforderlich oder möglich ist, eine Abmeldung im vorgenannten Sinne durchzuführen. Über eine solche Ausnahme entscheidet die eco Beschwerdestelle. Im Falle

[5] siehe http://www.dkim.org
[6] dreimonatige Übergangsfrist: verpflichtend ab 01.10.2019
[7] siehe auch http://en.wikipedia.org/wiki/VERP sowie http://www.list-unsubscribe.com
[8] siehe auch http://en.wikipedia.org/wiki/VERP sowie http://www.list-unsubscribe.com, dreimonatige Übergangsfrist: verpflichtend ab 01.10.2019

einer Ausnahme muss ein „List-Help"-Link (siehe RFC 2369)[9] in den Header eingefügt werden, wobei die ausschließliche Verwendung eines Mailto-Links im Rahmen der CSA nicht zulässig ist. Der Link muss zu einer Hilfe- oder Login-Seite führen, die dem Empfänger erklärt, wie er sich von einer weiteren Zusendung abmelden kann beziehungsweise weshalb dies aus zwingenden rechtlichen Gründen unter Benennung dieser Gründe nicht möglich ist.

2.19 Spätestens zwei Wochen nach erfolgter Zertifizierung muss der Versender einen „X-CSA-Complaints"-Header hinzufügen. Dieser Header darf nur vom letztendlich versendenden Mail Transfer Agent (MTA) gesetzt werden. Die Headerzeile lautet: „X-CSA-Complaints: whitelist-complaints@eco.de". Das Erfüllen dieses Kriteriums ist der CSA durch eine Testaussendung an „samples@certified-senders.org" zu bestätigen.

2.20 Sofern Redirect-Links verwendet werden, muss der Versender in der Lage sein, diese kurzfristig zu deaktivieren, um Redirect Abuse zu vermeiden. Bei einem Hinweis durch die Beschwerdestelle auf Phishing muss werktäglich spätestens nach 24 Stunden die Deaktivierung erfolgt sein.

2.21 Die Nutzung von „Whois Privacy"-Diensten, um die Identität des Domaininhabers zu verbergen, ist nicht zulässig.

Reputationskriterien

2.22 Der Versender muss E-Mail-Adressen von der Mailingliste nehmen, wenn nach dem Beschicken dieser Adressen die Nichtexistenz des Postfachs erkannt wird, spätestens jedoch, wenn drei Hard Bounces erfolgten.[10]

Insgesamt darf die Hard-Bounce-Rate grundsätzlich pro ISP 1,0 Prozent nicht übersteigen. Eine Ausnahme hiervon ist nur bei Neukunden möglich, sofern die zulässige Hard-Bounce-Rate lediglich einmalig überschritten wird.

2.23 Die Spam-Markierungsquote pro Mail-Server (IP-Adresse) beziehungsweise pro Email Service Provider (ESP) darf innerhalb einer Woche bei einem ISP 0,3 Prozent nicht übersteigen.

2.24 Der Versender darf keine wesentlichen Reputationsprobleme (IP- oder Domain-basiert) bei teilnehmenden ISP und Technologiepartnern (zum Beispiel basierend auf Spamtrap-Hits, Content-Scannern oder hohen Spamquoten) aufweisen.

3 Empfohlene Kriterien

3.1 Es wird dringend empfohlen, Nutzerdaten über das Internet über das so genannte Double-Opt-in(DOI)-Verfahren zu erheben, um den strengen Anforderungen der DSGVO bezüglich der Nachweispflicht gerecht zu werden. Das DOI im Sinne der CSA Vertragswerke beschreibt

[9] siehe auch http://en.wikipedia.org/wiki/VERP sowie http://www.list-unsubscribe.com
[10] E-Mail-Server Status Codes, die mit einer 5 beginnen, sind als Hard Bounce einzustufen, siehe zum Beispiel RFC 3463.

ein Verfahren, bei dem eine E-Mail, die die Einwilligung zum Beschicken mit E-Mails im Wortlaut wiedergibt (Bestätigungs-E-Mail), an die angemeldete E-Mail-Adresse gesendet wird und der Adressat die Einwilligung bestätigt, indem er auf diese Bestätigungs-E-Mail antwortet oder einen Link in der Bestätigungs-E-Mail anklickt. Erst nach Erhalt dieser Bestätigung des Adressaten ist der Versender berechtigt, die erhobene E-Mail-Adresse zu verwenden. Wird die Bestätigung nicht in angemessener Frist erteilt, so sind die im Zusammenhang mit der E-Mail-Adresse erhobenen Daten zu löschen. Ein Verfahren, bei dem in der Bestätigungs-E-Mail unter einem Vorwand (zum Beispiel bei Gewinnspielen eine Bestätigung der Adresse zum Zustellen von Gewinnen) lediglich die E-Mail-Adresse und nicht die explizite Einwilligung verifiziert wird, stellt kein DOI in diesem Sinne dar. Die Bestätigungs-E-Mail darf ansonsten keine werblichen oder sonstigen Inhalte umfassen. Die Versender verpflichten sich, dass von ihnen eingesetzte Verfahren nur beim Einhalten dieser Anforderungen als DOI zu bezeichnen.

3.2 Es wird empfohlen, schon bei der Bestellung von beispielsweise einem Newsletter über die voraussichtliche Frequenz der Mailings zu informieren, sofern eine Frequenz vorliegt oder geplant ist.

3.3 Darüber hinaus wird empfohlen, schon bei der Bestellung von beispielsweise einem Newsletter die versendenden E-Mail-Adressen anzugeben, damit der Adressat diese gegebenenfalls in sein Adressbuch aufnehmen kann.

3.4 Es wird empfohlen, dass für jede From-Absender-Adresse im Header (beziehungsweise deren E-Mail-Domain) von E-Mails ein unter Umständen zusätzlicher und eventuell mit niedrigster Priorität versehener MX-Record auf die absendende IP-Adresse existiert.

3.5 Es wird empfohlen, Versandaktionen von Neukunden ausschließlich über nicht in der Whitelist eingetragene Mail-Server abzuwickeln.

3.6 HTML-formatierte E-Mails sollten generell mit einem Text-Part (MIME) erweitert werden. Dieser sollte Abmeldeinformationen und Hinweise zum Newsletter enthalten, da Empfänger HTML-formatierte E-Mails nicht immer korrekt empfangen können.

3.7 Es wird empfohlen, eine valide Absender-Adresse einzusetzen, sodass der Adressat per „Antwort-Funktion" mit dem Absender Kontakt aufnehmen kann. Sollte dies nicht der Fall sein, wird empfohlen, mindestens eine valide Reply-to-Adresse einzusetzen.

3.8 Es wird empfohlen, Newsletter über andere IPs als Transaktions-Mails zu versenden.

3.9 Es wird empfohlen, Domain-based Message Authentication, Reporting and Conformance (DMARC) einzusetzen, sodass ISP als Empfänger entsprechend den vorgegebenen Parametern empfangene E-Mails prüfen können. Beim Einsatz von DMARC müssen Reporting-E-Mail-Adressen so angegeben sein, dass durch ISP versendete Reports bei dem zertifizierten Versender oder dessen Kunde(n) verarbeitet werden. Es wird empfohlen, eine „Reject"-Policy zu verwenden.

3.10 Die Einlieferung von E-Mails beim Empfänger sollte, sofern es der Empfänger unterstützt, über eine Transport Layer Security (TLS)-gesicherte Verbindung nach aktuellem Stand der Technik

erfolgen. Darüber hinaus sollte DANE[11] implementiert werden. Für den Versand von E-Mails ist bei der Prüfung der Zertifikate des Empfängers DNSSEC[12] nicht erforderlich. Ist DNSSEC voraussichtlich auch langfristig nicht verfügbar, sollte für die Absicherung eingehender E-Mails stattdessen bis dahin MTA-STS[13] eingesetzt werden.

3.11 Die Implementierung des „Form-Sub"-Headers[14] zur Erkennung von sogenannten „Mailbomb"-Attacken wird empfohlen.

3.12 Es wird empfohlen, DKIM-Schlüssel mit einer Länge von mindestens 1.024 Bit zu verwenden. Als Signaturalgorithmus sollte sha256 verwendet werden.

3.13 Es wird empfohlen, in versendeten E-Mails das Laden von externen Inhalten und Verbindungen zum Server nur über eine TLS-gesicherte Verbindung zuzulassen.

4 Rechtmäßigkeit

4.1 Der Versender ist dafür verantwortlich, dass der Versand rechtmäßig erfolgt und insbesondere die Inhalte der versendeten E-Mails nicht gesetzlichen Verboten und Geboten zuwiderlaufen.

4.2 Der Versender ist darüber hinaus dafür verantwortlich, dass mit jeder E-Mail auch sonstige Anforderungen für die rechtmäßige Umsetzung der in diesem Dokument niedergelegten Kriterien erfüllt sind. Dazu gehören beispielsweise Einwilligungen in das Versenden der anmeldenden IP-Adresse in einer zusätzlichen Header-Zeile.

5 Änderungsvorbehalt

eco behält sich vor, die Kriterien mit einer Ankündigungsfrist von sechs Wochen zu ändern. Dem zertifizierten Versender steht in diesem Fall ein außerordentliches Kündigungsrecht zu.

[11] DNS-based Authentication of Named Entities, siehe unter anderem https://tools.ietf.org/html/rfc7671
[12] Domain Name System Security Extensions, siehe https://www.denic.de/wissen/dnssec
[13] SMTP MTA Strict Transport Security, siehe https://tools.ietf.org/html/rfc8461
[14] siehe https://tools.ietf.org/html/draft-levine-mailbomb-header-01