Aufnahmekriterien

für die Teilnahme von Massenversendern an der Certified Senders Alliance (CSA)

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 Aufnahme von E-Mail-Versendern in die CSA.

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

2 Zwingende Aufnahmekriterien

2.1 Grundsätzlich werden alle von dem CSA-Versender genutzten IP-Adressen auf der Whitelist geführt. Die Nutzung von Mail-Servern, die nicht in der Whitelist eingetragen werden sollen, ist ausschließlich im folgenden Fall zulässig:

Bei Versandaktionen von Neukunden, wenn die Anzahl der Versandaktionen drei nicht übersteigt und 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 diese IP-Adressen auf die Whitelist gesetzt werden sollen oder nicht, sind die Namen und IP-Adressen sämtlicher vom Versender verwendeten E-Mail-Ausgangsserver zu benennen. Die Nutzung von E-Mail-Ausgangsservern, die nicht in die Whitelist eingetragen werden sollen, hat der Versender gegenüber der CSA explizit zu benennen.

Permission

2.2 Einwilligung

Der Versand von E-Mails erfolgt grundsätzlich nur an Adressaten, die hierzu ihre Einwilligung[1] erteilt haben (Opt-In). Die Einwilligung muss folgende Voraussetzungen erfüllen:

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

b. Sofern die Einwilligung nicht schriftlich oder elektronisch erklärt wird, bedarf sie einer schriftlichen Bestätigung gegenüber dem Adressinhaber.

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. Bereits 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 auch Informationen dazu enthalten, wie und gegenüber wem der Widerruf erfolgen kann. Die Möglichkeit des Widerrufs darf nicht komplizierter als die Einholung der Einwilligung gestaltet sein. Der erfolgte Widerruf muss nach spätestens fünf Werktagen umgesetzt sein.

2.3 Ausnahmsweise können auch ohne ausdrückliches Opt-In (vorherige Einwilligung, Ziffer 2.2) unter folgenden Voraussetzungen[3] E-Mails an Kunden versendet

1 Die benannten Einwilligungsvoraussetzungen entsprechen den Vorgaben der DSGVO.
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 für zwölf Monate ab Inkrafttreten dieser Aufnahmekriterien, im Beschwerdefall nicht zu einer Rüge führen.
3 Die Voraussetzungen entsprechen den Vorgaben von Art. 13 Abs. 2 der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG des Europäischen Parlamentes und des Rates vom 12. Juli 2002 und den nationalen Implementierungen.

werden:

a. Bestehende Kundenbeziehungen (Vorliegen eines entgeltlichen Austauschvertrags),

b. Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen,

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.

Gestaltung der E-Mail

2.4. Der Auftraggeber, das heißt der Vertragspartner des Versenders einer geschäftsmäßigen E-Mail, muss klar erkennbar sein. In jeder versendeten E-Mail muss ein leicht erkennbares Impressum[4], spätestens zwölf Monate nach Inkrafttreten der Aufnahmekriterien als Volltext, enthalten sein. Das Impressum muss die nachfolgenden Angaben enthalten:

a. den Namen und die Anschrift, unter der der Versender 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

c. eine Umsatzsteueridentifikationsnummer oder eine Wirtschaftsidentifikationsnummer, sofern vorhanden.

Weitergehende Informationspflichten nach nationalen Gesetzen bleiben unberührt.

2.5. Auf die Möglichkeit des Widerrufs der Erlaubnis, E-Mails zuzusenden, ist in jeder E-Mail hinzuweisen. Das Abbestellen von E-Mails muss grundsätzlich durch den Empfänger ohne Kenntnis von Zugangsdaten (beispielsweise Login und Passwort) möglich sein.

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))

Ausnahmen können im Einzelfall zugelassen werden, wenn eine abweichende Handhabung aufgrund von Besonderheiten des angebotenen Dienstes erforderlich ist; vergleiche Ziffer 2.21 bezüglich „List-Help".

2.6 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 die 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.

2.7 Beim Verwenden von E-Mail-Adressen, die der Versender beziehungsweise seine Kunden von Dritten erworben haben, gilt: Der Versender beziehungsweise sein Kunde muss sich vor der Vornahme von Werbehandlungen vergewissern, dass eine Einwilligung im Sinne dieser Aufnahmekriterien vorliegt. Diese Einwilligung muss sich explizit auch auf den Versender beziehungsweise seinen Kunden beziehen.

2.8 Die Gewinnung von Adressdaten für Dritte (etwa durch Co-Sponsoring) muss gegenüber dem Nutzer transparent sein. Insbesondere dürfen so gewonnene Adressdaten nur für eine Versendung genutzt werden, wenn bei der Erhebung

a. die Unternehmen, für die die Adressdaten generiert wurden, transparent, namentlich und unter Angabe der Branche einzeln benannt wurden,

b. die Kenntnisnahme der Liste der Unternehmen für den Nutzer leicht und eindeutig möglich war und

c. die Anzahl der Unternehmen beziehungsweise Personen, für die die Adressdaten erhoben wurden, auf ein Maß reduziert ist, 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.

Technische Konfiguration

2.9 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.).

2.10 Jede versendete E-Mail (Aufbau und Komposition) sowie der E-Mail-Versand (Envelope-Kommunikation im SMTP-Dialog) müssen RFC-konform sein.

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

2.11 Die IP-Adresse des versendenden Mail-Servers beziehungsweise die IP-Adresse, die eine E-Mail an den Internet Service Provider 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 (ARR) 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).

2.12 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).

2.13 Der Versender hat eine unter Umständen separate Abuse-/Complaint- beziehungsweise Feedback-Loop-E-Mail-Adresse (frei definierbarer ROLE Account, der beim Versender für die Zusendung von unter Umständen automatisierten Beschwerden oder Anfragen von ISPs oder Empfängern zuständig ist) für die von ihm verwendeten IP-Adressen einzurichten und der CSA zu benennen. Die Fähigkeit zur Verarbeitung von ARF (siehe RFC5965) und X-ARF[5] wird vorausgesetzt. Darüber hinaus sind Ansprechpartner mit Telefonnummer und E-Mail-Adressen für Beschwerden zu benennen. Die Reaktionszeit bei Anfragen von ISPs darf maximal 24 Stunden werktäglich betragen.

5 siehe http://www.x-arf.org

2.14 Der Versender muss die alleinige Kontrolle über die versendenden Mail-Server haben.

2.15 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.

2.16 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.[6]

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 einmalig überschritten wird.

2.17 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.

2.18 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.

2.19 Bezüglich der in der Envelope-Kommunikation zwischen E-Mail-Servern angegebenen MAIL-FROM-Adresse müssen für deren Domain-Namen-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.

2.20 Das Verfahren DomainKeys Identified Mail (DKIM)[7] 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

6 E-Mail-Server Status Codes, die mit einer 5 beginnen, sind als Hard Bounce einzustufen. siehe zum Beispiel RFC 3463

7 siehe http://www.dkim.org

„From“, „X-CSA-Complaints“ und „List-Unsubscribe“ umfassen.

2.21 In den Header der E-Mail muss ein „List-Unsubscribe"-Link (siehe RFC 2369)[8] eingefügt werden, wobei die ausschließliche Verwendung eines Mailto-Links im Rahmen der CSA nicht zulässig ist. Die angegebenen Links müssen eine erleichterte One-Click-Abmeldung mindestens auf Listenebene bewirken. Der Versender kann dem Nutzer eine Bestätigungs-E-Mail für eine erfolgte Abmeldung übersenden. Verpflichtend ab dem 01.07.2019 muss zusätzlich RFC 8058[9] implementiert werden, um dem Empfänger die One-Click-Funktionalität zu signalisieren.

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, die auch für CSA-Beschwerden zuständig ist. Im Falle einer Ausnahme muss ein „List-Help-Link“ (siehe RFC 2369)[10] 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.

2.22 Spätestens zwei Wochen nach erfolgter Zertifizierung ist vom Versender ein „X-CSA-Complaints“-Header hinzuzufügen. Die Headerzeile lautet: „X-CSA-Complaints: whitelist-complaints@eco.de“. Das Erfüllen dieses Kriteriums ist der CSA durch eine Testaussendung an „samples@certifiedsenders.eu“ zu bestätigen.

2.23 Sofern Redirect-Links verwendet werden, muss der CSA-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.

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

8 siehe auch http://en.wikipedia.org/wiki/VERP sowie http://www.list-unsubscribe.com
9 siehe https://tools.ietf.org/html/rfc8058
10 siehe auch http://en.wikipedia.org/wiki/VERP sowie http://www.list-unsubscribe.com

3 Empfohlene Aufnahmekriterien / Double-OPT-IN

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

3.5 Es wird empfohlen, dass für jede From-Absende-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.

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

3.7 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.

3.8 Es wird empfohlen, eine valide Absender-Adresse einzusetzen, so dass 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.

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

3.10 Es wird empfohlen, DMARC einzusetzen, so dass 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.

3.11 Die Einlieferung von E-Mails beim Empfänger sollte, sofern es der Empfänger unterstützt, über eine TLS-gesicherte Verbindung nach aktuellem Stand der Technik erfolgen.

3.12 Die Implementierung des „Form-Sub"-Headers[11] zur Erkennung von sogenannten „Mailbomb"-Attacken wird empfohlen.

11 siehe https://tools.ietf.org/html/draft-levine-mailbomb-header-01

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 Massenversender steht in diesem Fall ein außerordentliches Kündigungsrecht zu. Im Falle der Kündigung werden gezahlte Beiträge anteilig erstattet.