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 Mailbox- und Security-Providern zum Aufrechterhalten der Netzwerksicherheit und Dienststabilität eine Zustellung verhindern können.

2 Zwingende Kriterien

2.1 Benennung von IP-Adressen

a. Der zertifizierte Versender muss die Namen und IP-Adressen aller genutzten E-Mail-Ausgangsserver gegenüber der CSA/eco benennen.

b. Grundsätzlich werden alle vom zertifizierten Versender benannten IP-Adressen auf der Certified IP List geführt. Eine Ausnahme hiervon ist ausschließlich für die ersten drei Versandaktionen von Neukunden zulässig, sofern 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.

Rechtliche Kriterien

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 Produkte, für die geworben werden soll, müssen klar und verständlich angegeben sein.

c. Die Einwilligung Minderjähriger ist nur wirksam, 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,

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 durch den Kunden erfolgt.

---

[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. Juli 2021, im Beschwerdefall nicht zu einem Hinweis führen.

[3] Die Voraussetzungen entsprechen den Vorgaben von Artikel 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.

2.4 Datenerhebung durch Dritte (etwa durch Co-Sponsoring)

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.

Gestaltung der E-Mail

2.5 Der zertifizierte Versender beziehungsweise dessen 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

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

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

können im Einzelfall durch die eco Beschwerdestelle zugelassen werden, wenn eine abweichende Handhabung aufgrund von Besonderheiten des angebotenen Dienstes erforderlich ist.

2.7 In den Kopfzeilen der E-Mail (zum Beispiel Betreff, Absendername) darf der kommerzielle Charakter der Nachricht nicht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn Kopfzeilen 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 Kriterien

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 betreffenden Request for Comments (RFC) der IETF sein.

Maßgebend sind die jeweils aktuellen RFC. Zum Zeitpunkt der Erstellung dieses Dokuments sind das unter anderem RFC 6532, 2142, 2369, 5321, 5322 und 5335.

2.10 Die Einlieferung von E-Mails beim Empfänger muss über eine „Transport Layer Security (TLS)"-gesicherte Verbindung nach aktuellem Stand der Technik erfolgen.

2.11 Die IP-Adresse des versendenden Mail-Servers muss im Reverse-Lookup via PTR zu mindestens einem Fully Qualified Domain Name (FQDN nach RFC 4703) auflösen. Der FQDN muss im Umkehrschluss im A-Record die IP-Adresse des versendenden Mail-Servers enthalten. Der FQDN muss im SMTP-Dialog (Envelope) beim HELO/EHLO-Kommando angegeben werden. Der FQDN darf nicht die IP-Adresse des Servers enthalten (zum Beispiel server-80-12-54-125.example.org oder server126.net80-12-54.example.org).

Darüber hinaus muss der FQDN in seiner Bezeichnung als Server einer Infrastruktur zum Versenden von Massen-E-Mails erkennbar und lesbar sein und darf nicht durch eine verschleiernd, alphanumerisch kodierte Kennung ähnlich wie ein Dial-up Service aussehen.
Es gilt eine Übergangsfrist für bestehende Zertifizierungen bis zum 01.09.2022.

2.12 Der Versender ist verpflichtet, eine allgemeine Abuse-E-Mail-Adresse (abuse@org-domain.tld)[5] einzurichten und zu überwachen.
Es gilt eine Übergangsfrist bis zum 01.09.2022 für zertifizierte Versender.

2.13 Der Versender muss die alleinige Verantwortung über die versendenden E-Mail-Server haben. Zum Nachweis muss der Versender einen eindeutigen, von der CSA bereitgestellten, Token[6] als TXT Eintrag in der DNS des jeweiligen Hostnames (FQDN) anlegen und für den Zeitraum

[5] siehe unter anderem RFC 2142, Sender Complaint Handling der M3AAWG und andere aktuelle Richtlinien/Best Practices der Regional Internet Registries [RIR] und anderer Registries
[6] Ausgabe des Tokens für bereits zertifizierte Versender erfolgt im Zeitraum 04-2022 bis 06-2022

der Zertifizierung als stetigen Nachweis belassen. Der TXT Eintrag im FQDN des E-Mail Servers muss die folgende Syntax erfüllen: `CSA-certified-host=<token>.` Der Versender übernimmt damit die vollständige Verantwortung für den E-Mail-Verkehr, der über diesen E-Mail-Server (IP und FQDN des Hosts) versendet wird.

Es gilt eine Übergangsfrist bis zum 01.10.2022.

2.14 Die vom Versender benannten E-Mail-Ausgangsserver dürfen nur für den automatisierten Versand von Massen-E-Mails oder sogenannten transaktionalen E-Mails verwendet werden. Idealerweise muss es möglich sein, spezifische Kampagnen bestimmten dedizierten Systemen zuzuordnen.

2.15 Für die in der SMTP-Kommunikation zwischen E-Mail-Servern angegebene MAIL-FROM-Adresse ist ein SPF-Eintrag anzulegen. Dieser dient der Authentifizierung des versendenden E-Mail-Servers gegenüber dem empfangenden E-Mail-Server. Der SPF-Eintrag muss mit „-all" oder „~all" enden.

2.16 Zur Verarbeitung von Bounces, die während der SMTP-Kommunikation auftreten können, muss für die From-Domain in der Envelope-Kommunikation ein MX-Record angegeben werden. Als Alternative (Fall-Back) ist ein A-Record zulässig.

2.17 In jeder versendeten E-Mail muss entweder ein „List-Unsubscribe"-Header oder ein „List-Help"-Header (siehe RFC 2369)[7] enthalten sein. Der „List-Unsubscribe"-Header ist für listenbasierte Mailings erforderlich und mit „POST HTTPS"-Link inklusive „One-Click-Unsubscribe"-Funktionalität (RFC 8058)[8] einzufügen. Der angegebene Link muss eine direkte One-Click-Abmeldung mindestens auf Listenebene bewirken. Der Versender darf dem Nutzer eine Bestätigungs-E-Mail für die erfolgte Abmeldung übersenden.

Bei nicht-listenbasierten Mailings muss alternativ zum „List-Unsubscribe"-Header der „List-Help"-Header gesetzt werden. Der „List-Help"-Header muss mindestens eine „mailto:"-Adresse oder einen HTTPS-Link enthalten, HTTP-Links sind nicht zulässig. Sowohl die Verwendung der „mailto:"-Adresse als auch des HTTPS-Links müssen dem Empfänger die Möglichkeit geben, Informationen zu erhalten, aus welchem Grund die E-Mail an ihn versendet wurde und weshalb eine Abmeldung auf Listenebene nicht möglich ist.

Sollte der zertifizierte Versender weder den „List-Unsubscribe"-Header noch den „List-Help"-Header einbinden können, muss dies bei der eco Beschwerdestelle begründet und durch diese als Ausnahme genehmigt werden. Hierzu genügt eine formlose E-Mail an csa-complaints@eco.de.

2.18 Ab erfolgter Zertifizierung ist ein „X-CSA-Complaints"-Header einzufügen. Hierfür wird eine Umsetzungsfrist von zwei Wochen gewährt, die mit erfolgter Zertifizierung beginnt. Die Headerzeile lautet: „X-CSA-Complaints: csa-complaints@eco.de" und darf nur vom letztendlich versendenden Mail Transfer Agent (MTA) gesetzt werden. Das Erfüllen dieses Kriteriums ist der CSA durch eine Testaussendung an „samples@certified-senders.org" zu bestätigen. Der „X-

[7] siehe auch http://en.wikipedia.org/wiki/VERP
[8] siehe auch http://en.wikipedia.org/wiki/VERP

CSA-Complaints"-Header muss in DKIM-signiert werden (siehe 2.20).

2.19 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 eco Beschwerdestelle auf Phishing muss werktäglich spätestens nach 24 Stunden die Deaktivierung erfolgt sein.

2.20 Jede ausgehende E-Mail muss mit einer validen DKIM-Signatur (DomainKeys Identified Mail) versehen sein. Die im „d="-Tag verwendete Domain muss via WHOIS-Eintrag entweder dem Versender oder dem Kunden des Versenders zugeordnet werden können.

Mindestens die Header-Elemente "From", "X-CSA-Complaints", "List-Unsubscribe und List-Unsubscribe-Post" oder "List-Help" müssen DKIM-signiert sein.

2.21 Alle Nachrichten eines Versenders müssen ein DKIM Alignment enthalten. DKIM Alignment bedeutet die mindestens relaxte Übereinstimmung des "d="-Tags mindestens einer DKIM-Signatur mit der Domain aus dem From Header (RFC5322), mindestens auf organisatorischer Ebene.

Beispiel:

```
DKIM-Signature: v=1; ...; d=example.com; ...
From: "Example" <sender@child.example.com>
```

Es gilt eine Übergangsfrist bis zum 01.03.2023.

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.[9]

Die durchschnittliche Hard-Bounce-Rate pro Mail-Server (IP-Adresse) beziehungsweise pro E-Mail-Versender darf innerhalb des Zeitraums von sieben Tagen (einer Woche) bei einem Mailbox-Provider 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-Markierungsrate pro Mail-Server (IP-Adresse), pro DKIM-Domain beziehungsweise pro E-Mail-Versender darf innerhalb des Zeitraums von sieben Tagen (einer Woche) bei einem Mailbox-Provider 0,3 Prozent nicht übersteigen. Die Spam-Markierungsquote ergibt sich aus dem Verhältnis der Anzahl von Spam-Beschwerden durch die Empfänger zu der Anzahl der E-Mails im Posteingang.

2.24 Der Versender darf keine wesentlichen Reputationsprobleme (IP- oder DKIM-basiert) bei teilnehmenden Mailbox- oder Security-Providern (zum Beispiel basierend auf Spamtrap-Hits, Content-Scannern oder hohen Spamquoten) aufweisen.

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

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 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 Certified IP List 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 Ein Versender sollte DANE[10] implementieren. Für den Versand von E-Mails ist bei der Prüfung der Zertifikate des Empfängers DNSSEC[11] nicht erforderlich. Ist DNSSEC voraussichtlich auch langfristig nicht verfügbar, sollte für die Absicherung eingehender E-Mails stattdessen bis dahin MTA-STS[12] eingesetzt werden.

3.11 Die Implementierung des „Form-Sub"-Headers[13] 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.

3.14 Aus Gründen der Transparenz gegenüber dem E-Mail-Empfänger wird empfohlen, keine URL-Shortener zu verwenden.

3.15 Des Weiteren wird dringend empfohlen, das DKIM Alignment (siehe Kriterium 2.21) auf den Mail-From-Header (RFC5321) auszuweiten.

Beispiel:

```
DKIM-Signature: v=1; ...; d=example.com; ...
MAIL FROM: <xyz@foo.example.com>
From: "Example" <sender@child.example.com>
```

Darüber hinaus bietet es sich an, auch für die List-Header (RFC4021), Reply-To-Header (RFC5322), sowie wenn vorhanden Sender-Header (RFC5322), mit einer oder der gleichen DKIM Signatur, ebenfalls auf organisatorischer Ebene, eine Übereinstimmung herbeizuführen.

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.

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.

---

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