Criteria

Pertaining to the Participation of Email Senders
in the Certified Senders Alliance (CSA) – CSA Criteria

1 Preamble

This document describes the criteria for participation of email senders in the CSA as jointly defined by eco – Association of the Internet Industry (eco) and Deutscher Dialogmarketing Verband e.V. (DDV) [German Dialogue Marketing Association].

Meeting the criteria laid down here does not guarantee that emails will be delivered to the intended users, since their filter settings or measures from mailbox and security providers to maintain network security and the stability of services may prevent delivery to the user.

2 Mandatory Criteria

2.1 Provision of IP Addresses

a. The certified Sender must provide the CSA/eco with the names and IP addresses of all outbound email servers.

b. In principle, all IP addresses provided by the certified Sender are placed on the Certified IP List. An exception to this rule is only permitted for the first three mailing campaigns of new customers, provided that no more than two months have passed since the time of the first mailing campaign. A mailing campaign is defined as the sending of an email with predominantly the same content to a pre-defined group of recipients.

Legal Criteria

Permission

2.2 Consent

Emails (marketing emails/newsletters) may, in principle, only be sent to recipients who have provided their consent to this[1] (Opt-In). The consent must comply with the following prerequisites:

a. Consent must be granted actively and separately. The recipient must either click/check a box or otherwise similarly declare their clear agreement. This declaration may not form part of any other declarations (e.g. consent to general terms and conditions of business, general data protection provisions) and may only relate to advertising.

b. Consent must be given for the specific context and in an informed manner. The beneficiary of the consent must be explicitly named. The sector and the products for which marketing emails are to be sent must be provided clearly and understandably.

c. Consent of minors is only valid if:
- the minor has reached the age of 16 years, or
- the legal guardians have given consent.[2]

d. The option to revoke consent at any time with future effect must be clearly and explicitly indicated at the time of obtaining consent. This must also contain information as to how consent may be revoked and with whom. The option to revoke consent may not be more complicated than the obtaining of the consent. Revoked consent must be implemented after five (5) working days at the latest.

2.3 On an exceptional basis, emails may also be sent to customers without explicit Opt-in (see 2.2) under the following conditions:[3]

a. Existing customer relationship (existence of an exchange contract in return for payment),

b. Direct advertising for similar proprietary products or services,

c. Information about the option to object at any time (when obtaining and with each use

[1] The requirements specified for consent are in accordance with the provisions of the General Data Protectio Regulation (GDPR) and the Data Protection Directive for Electronic Communication 2002/58/EC of the European Parliament and of the Council dated 12 July 2002, as well as the national implementations.

[2] This provision is based on the GDPR. At present, no implementation guideline can be offered. Therefore, in the event of a complaint concerning a breach of this requirement, no notification will ensue until clarification has occurred with the data protection authorities – in any case, at least until 1 July 2021.

[3] The prerequisites are in accordance with the provisions of Art. 13 (2) of the Data Protection Directive for Electronic Communication 2002/58/EC of the European Parliament and of the Council dated 12 July 2002, as well as the national implementations.

of the email address), without incurring any costs arising other than transmission costs at basic rates, and

d. The customer has not objected.

2.4 Data collection by third parties (e.g. through co-sponsoring)

When using email addresses that the Sender or the Sender's customer has acquired from third parties, the following applies:

a. Before carrying out marketing measures, the Sender or the Sender's customer must ensure that a consent declaration (see Point 2.2) exists. This consent declaration must also refer explicitly to the Sender or the Sender's customer.

b. During the collection of the data the list of beneficiaries must be easy to understand and unambiguous for the user.

c. The number of companies or individuals for whom the address data is collected has been/was reduced to a volume which precludes the forwarding of the user data to a disproportionately large group of third parties. The number must enable the user to easily grasp the significance and the scope of their consent, and to easily monitor the legal handling of their data.

In the interest of clarity, it must be pointed out that the companies for whom the address data has been generated are not permitted to forward this address data to third parties without especially gaining a further consent declaration from the user.

Design of the Email

2.5 The certified Sender or its contracting entity – that is, the Sender's contractual partner – must be clearly identifiable. In every business email sent, an easily recognizable legal notice (footer)[4] must be contained as full text. The legal notice must contain the following details:

a. The name and address of where the Sender is established; for legal entities also the legal structure, the commercial register, the association register, partnership register or the register of cooperatives in which they are recorded, and the applicable register number,

b. contact information, at least one valid telephone number or an electronic contact form, and an email address and

c. a sales tax identification number or a business identification number, if applicable.

Further obligations to provide information in accordance with national laws are not affected.

2.6 The option to revoke permission to send emails (Opt-out) must be indicated in every email.

[4] Legal notice under the terms of Article 5 (1) of the EU E-Commerce Directive 2000/31/EC and the national implementations (e.g. Germany Section 5 (1) of the Telemedia Act (Telemediengesetz –TMG)

Unsubscribing from emails must always be possible without the recipient having to know any access data (for example, login and password). Exceptions can be granted by the eco Complaints Office in individual cases if different handling is required due to certain particularities of the service offered.

2.7 The commercial nature of the message may not be obfuscated or concealed in the header of the email (for example, subject line, Sender's name). An obfuscation or concealment occurs when headers are intentionally designed such that the recipient, prior to viewing the content of the communication, receives either no information or misleading information about the actual identity of the Sender or the commercial nature of the message.

Technical Criteria

2.8 The Sender's servers must be adequately technically secure (e.g. firewall, no open relay, no public proxy, no backscatter, continuously monitored servers, etc.).

2.9 Every email sent (layout and composition) and email transmission (envelope communication in SMTP dialog) must conform to the relevant Request for Comments (RFC) of the IETF.

The current RFCs are decisive. At the time of creating this document, these include the RFCs 6532, 2142, 2369, 5321, 5322 and 5335.

2.10 Emails to the recipient must be delivered via a Transport Layer Security (TLS)-secured connection, in accordance with the current level of technology.

2.11 The IP address of the outbound mail server must be able to resolve in Reverse-Lookup via PTR to at least one Fully Qualified Domain Name (FQDN pursuant to RFC 4703). In the reverse resolve, the FQDN used must contain the IP address of the outbound mail server in the A-record. The FQDN must be specified in the SMTP dialog (envelope) for the HELO/EHLO command. The FQDN must not contain the server's IP address (e.g. server-80-12-54-125.example.org or server126.net80-12-54.example.org).

Furthermore, the FQDN must be recognizable and readable in its designation as a server of an infrastructure for sending mass emails and should not resemble a dial-up service by means of an obfuscating, alphanumerically coded identifier.
A transition period for existing certifications applies until 01 September 2022.

2.12 The Sender is obliged to set up and monitor a general abuse email address (abuse@org-domain.tld).[5]

A transition period for certified Senders applies until 01 September 2022.

2.13 The Sender must have sole responsibility over the outbound email servers.

[5] See, among others, RFC 2142, the M3AAWG's Sender Complaint Handling, and other current guidelines/best practices of the Regional Internet Registries [RIR] and other registries.

As evidence of this, the Sender must create a unique token[6] provided by the CSA as a TXT entry in the DNS of the respective host name (FQDN), and must maintain this as consistent evidence for the period of certification. The TXT entry in the FQDN of the email server must comply with the following syntax: `CSA-certified-host=<token>.` In so doing, the Sender assumes full responsibility for the email traffic sent via this email server (IP and FQDN of the host).

A transition period until 01 October 2022 applies.

2.14 The outbound email servers specified by the Sender may only be used for the automated sending of bulk mailings or for what are called transactional emails. Ideally, it must be possible to assign specific campaigns to certain dedicated systems.

2.15 An SPF record must be entered in the MAIL FROM address specified in the SMTP communication between the email servers. This allows for authentication of the outbound email server vis-à-vis the recipient email server. The SPF record must end with "-all" or "~all".

2.16 To handle bounces that may occur during SMTP communication, an MX record must be specified for the "From" domain in the envelope communication. As an alternative (Fall-Back), an A-record is permitted.

2.17 Each email sent must incorporate either a "List-Unsubscribe" header or a "List-Help" header (see RFC 2369).[7] The "List-Unsubscribe" header is required for list-based mailings and must be inserted with a "POST HTTPS" link including "One-Click-Unsubscribe" functionality (RFC 8058).[8] The specified links must enable a direct one-click unsubscribe, at least at list level. The Sender may send a confirmation email to the user when successfully unsubscribed.

For non-list-based mailings, the "List-Help" header must be set as an alternative to the "List-Unsubscribe" header. The "List-Help" header must contain at least a "mailto:" address or a HTTPS link; HTTP links are not permitted. Both the "mailto:" address and the HTTPS link must allow the recipient to receive information about the reason why the email was sent to them and why it is not possible to unsubscribe at list level.

If the certified Sender is unable to include either the "List-Unsubscribe" header or the "List-Help" header, the reason for this must be reported to the eco Complaints Office and approved by them as an exception. An informal email to csa-complaints@eco.de suffices for this purpose.

2.18 Once certification is complete, an "X-CSA-Complaints" header must be inserted. A two-week implementation period is granted for this, beginning after successful certification. The header line should read: "X-CSA-Complaints: csa-complaints@eco.de" and may only be set by the mail transfer agent (MTA) that is ultimately sending the message. The fulfilment of this criterion must be confirmed to the CSA by sending a test mail to "samples@certified-senders.org". The "X-

[6] The token for existing certified senders will be issued in the period 04-2022 to 06-2022
[7] See also http://en.wikipedia.org/wiki/VERP
[8] See also http://en.wikipedia.org/wiki/VERP

CSA-Complaints" header must be signed in DKIM (see 2.20).

2.19 If redirect links are used, the certified Sender must be able to deactivate them at short notice in order to avoid redirect abuse. In the event of a notification of phishing by the eco Complaints Office, the deactivation must be completed at the latest within 24 hours on work days.

2.20 Every outbound email must be assigned with a valid DKIM signature (domain keys identified mail). The domains used in the "d=" tag must point via a WHOIS record either to a Sender or a customer of the Sender.

At a minimum, the header elements "From", "X-CSA-Complaints", "List-Unsubscribe" and "List-Unsubscribe-Post" or "List-Help" must be DKIM-signed.

2.21 All messages from a Sender must contain a DKIM Alignment. DKIM Alignment means using, at a minimum, the relaxed alignment of the "d=" tag of at least one DKIM signature with the domain contained in the From Header (RFC5322), with this to be conducted at least on an organizational level.

For example:

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

A transition period until 01 March 2023 applies.

Reputation Criteria

2.22 The Sender must remove an email address from the mailing list when, after sending to this address, the non-existence of this inbox is determined, but at the latest after three hard bounces.[9]

The average hard bounce rate per mail server (IP address) or per email Sender must not exceed 1.0 percent within a seven-day (one week) period at a mailbox provider. An exemption from this rule is only possible for new customers, as long as the permissible hard-bounce rate is exceeded once only.

2.23 The spam click rate per mail server (IP address), per DKIM domain, or per email Sender must not exceed 0.3 percent within a seven-day (one week) period at a mailbox provider. The spam click rate is calculated on the basis of the ratio of the number of spam complaints by the recipients to the number of emails in the inbox.

2.24 There must be no evidence of the Sender having unacceptable reputation problems (IP- or DKIM-based) at participating mailbox or security providers (e.g. based on spamtrap hits, content scanners and high spam rates).

[9] E-Mail-Server Status Codes that begin with a 5 are to be categorized as hard bounces. See e.g. RFC 3463.

3 Recommended Criteria

3.1 It is strongly recommended that, when obtaining user data via the Internet, this is conducted using the so-called "Double-Opt-In-Procedure" (DOI) in order to meet the strict requirements of the GDPR regarding burden of proof. The DOI under the terms of the CSA agreements describes a process whereby an email, which thereupon reflects consent for emails to be sent (confirmation email), is sent to the registered email address and the recipient grants consent by responding to this confirmation email or clicking a link in the confirmation email. Only after this confirmation is received from the recipient is the Sender entitled to use the email address obtained. If confirmation is not provided within a reasonable period of time, the data obtained relating to the email address must be deleted. A procedure by which solely the email address and not the explicit consent is verified in the confirmation email under a pretext (e.g. for competitions, confirmation of the address for awarding prizes) does not represent a DOI in this sense. Apart from that, the confirmation email may not contain any advertising or other content. The Sender agrees to only describe the procedures implemented by them as DOI if they comply with these requirements.

3.2 As soon as a newsletter, for example, is requested, it is recommended that information regarding the expected frequency of mailings is provided, if a frequency has been set or is planned.

3.3 In addition, as soon as a newsletter, for example, is requested, it is also recommended that the outbound email address be provided in order to enable the recipient to record this in their address book.

3.4 It is recommended that an additional MX record should exist as required on the outgoing IP address, potentially allocated lowest priority, for each From Sender address (i.e. its email domain) in the header of emails.

3.5 The exclusive handling of mailing campaigns for new customers via non-listed mail servers is recommended.

3.6 HTML-formatted emails should usually be extended with a text part (MIME). This should contain information on unsubscribing and notes about the newsletter, since recipients may not always receive HTML-formatted emails correctly.

3.7 Incorporating a valid Sender address, so that the recipient can contact the Sender using the reply function, is recommended. If this is not done, incorporating at least a valid reply-to address is recommended.

3.8 It is advisable to send newsletters via other IPs than transactional emails.

3.9 Implementing Domain-based Message Authentication, Reporting and Conformance (DMARC) is recommended so that ISPs as recipients may check received emails in accordance with the

prescribed parameters. When implementing DMARC, reporting email addresses must be specified such that reports sent by ISPs are processed by the certified Sender or its customer(s). Putting a reject-policy in place is recommended.

3.10 A Sender should implement DANE. When sending emails, DNSSEC[10] is not required when checking the certificate of the receiver. If DNSSEC is not likely to be available for the foreseeable future, MTA-STS[11] should be used instead to secure incoming emails in the meantime.

3.11 To facilitate the detection of so-called "mailbomb" attacks, the implementation of the "Form-Sub" header[12] is recommended.

3.12 Using a DKIM key with a length of at least 1024 Bit is recommended. sha256 should be used as the signature algorithm.

3.13 It is recommended that the loading of external content and connections in sent emails to the server should only be permitted over a TLS connection.

3.14 For reasons of transparency vis-à-vis the e-mail recipient, the use of URL-shorteners is not recommended.

3.15 Furthermore, it is strongly recommended to extend the DKIM alignment (see criterion 2.21) to the Mail From header (RFC5321).

Example:

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

In addition, it is advisable to also create a match for the List Header (RFC4021), the Reply-to Header (RFC5322), and (if available) the Sender Header (RFC5322) with one or the same DKIM signature, likewise at the organizational level.

4 Lawfulness

4.1 The Sender is responsible for the mailing being performed lawfully and, in particular, for ensuring that the content of the sent emails does not contravene legal rules and restrictions.

4.2 In addition, the Sender is responsible for ensuring compliance with other legal requirements for the lawful implementation of the criteria as stated in this document.

[10] Domain Name System Security Extensions, see https://www.denic.de/wissen/dnssec/
[11] SMTP MTA Strict Transport Security, see https://tools.ietf.org/html/rfc8461
[12] See https://tools.ietf.org/html/draft-levine-mailbomb-header-01

5 Reservation of Right to Modification

eco reserves the right to modify the criteria giving a notice period of six weeks. In this case, the certified Sender shall have the right of extraordinary termination.