



Admission Criteria

Pertaining to the Participation of Bulk Mailers
in the Certified Senders Alliance (CSA)

1 Preamble

This document describes the admission criteria for bulk mailers into the CSA as jointly defined by eco - Verband der Internetwirtschaft e.V. (eco) [Association of the Internet Industry] and Deutscher Dialogmarketing Verband e.V. (DDV) [German Dialogue Marketing Association].

Meeting the criteria laid down here does not ensure that emails are delivered to the intended users since their filter settings or measures from Internet service providers to maintain network security and the stability of services may prevent delivery to the user.

2 Mandatory Admission Criteria

2.1 In principle, all IP addresses used by the CSA mailer are listed on the whitelist. Using mail servers that are not to be whitelisted is only permitted in the following case:

- Mailing campaigns from new customers, if the number of mailings does not exceed three (3) and no more than two (2) months have passed since the first mailing campaign. A mailing campaign is defined as the transmission over one time period of predominantly the same email content to a pre-defined group of recipients.

Irrespective of whether these IP addresses should be placed on the whitelist or not, the names and IP addresses of all outbound email servers used by the mailers must be specified. The use of outbound email servers that are not to be whitelisted must be explicitly specified by the mailer to the CSA.

Permission

2.2 Consent

Emails may, in principle, only be sent to recipients who have provided their consent to this¹ (opt-IN). The consent must comply with the following prerequisites:

a. Consent to receiving advertising material via email/newsletter must, in particular, be granted actively and separately. The recipient must either click/check a box or otherwise similarly declare his/her 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 via electronic mail.

b. If consent is not granted in writing or electronically, it requires written confirmation from the address holder.

c. The option to revoke consent at any time with future effect must be 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 exceptions basis, emails may also be sent to customers without explicit opt-in (prior consent, point 2.2) under the following conditions:²

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

d. The customer has not objected.

Email format

2.4 The contracting entity, that is the mailer's contractual partner for the advertising mail, must be clearly recognizable. Every email sent must contain an easily recognizable legal notice,³ either in the text or accessible via a direct link. The legal notice must contain the following details:

¹ The requirements specified for consent are in accordance with the provisions of Art. 13 para. 1 of the Data Protection Directive for Electronic Communication 2002/58/EC and national implementations (for an overview of the individual national implementations, see Annex 1)

² The prerequisites are in accordance with the provisions of Art. 13 para. 2 of the Data Protection Directive for Electronic Communication 2002/58/EC of the European Parliament and of the Council dated July 12, 2002 and with national implementations (for an overview of the individual national implementations, see Annex 1)

³ Legal notice under the terms of Article 5 para. 1 of the EU E-Commerce Directive 2000/31/EC and national implementations (e.g. in Germany § 5 para. 1 of the Telemedia Act (Telemediengesetz [TMG])

- a. The name and address where the mailer is domiciled; for legal entities also the legal structure, the authorized representatives and the commercial register, 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;
- c. Where a sales tax identification number or a business identification number is available, details of this number.

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

- 2.5 The option to revoke permission to send emails must be indicated in every email. 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 in individual cases if different handling is required due to certain particularities of the service offered; see point 2.21 concerning "list help".
- 2.6 The sender and the commercial nature of the message may not be obscured or hidden in the header and subject line of the email. This is the case when the header and subject line have been intentionally designed such that the recipient has no or misleading information about the actual identity of the sender or the commercial nature of the message prior to viewing the content of the communication.
- 2.7 When using email addresses that the mailer or their customer have acquired from third parties, the mailer and/or their customer are obliged prior to carrying out advertising activities to ensure that only those recipients are actually contacted, who have granted consent under the terms of these Admission Criteria. This consent has to refer not only to mailing by a third party but also by the mailer and/or their customer.

- 2.8 Obtaining address data for third parties (for instance via co-sponsoring) must be transparent to the user. In particular, address data obtained in this way may only be used for a mailing, if, when collecting:
- a. The companies, for which the address data was generated, were transparently and individually named with details of the sector,
 - b. The user was easily and clearly able to be aware of the list of companies and
 - c. The number of companies and/or persons for which the address data was collected is reduced to an extent that excludes forwarding user data to a disproportionately large number of third parties and permits the user to easily grasp the significance and scope of their consent and to easily monitor the lawful handling of their data.

In the interest of clarity, it must be pointed out that the companies, for which the address data was generated, may not forward this data to third parties without the user having separately provided additional consent to this.

Technical Configuration

- 2.9 The mailer's servers must be adequately secure (e.g. firewall, no open relay, no public proxy, no backscatter, continuously monitored servers, etc.).
- 2.10 Every email sent (layout and composition) and email transmission (envelope communication in SMTP dialog) must be RFC compliant.
- Current RFCs regarding SMPT, among other things, apply. At the time of creating this document, these include 2045 - 2048, 2142, 5321, 5322, 5335.
- 2.11 The IP address of the outbound mail server or the IP address that delivers an email to the Internet service provider must be able to reverse resolve via PTR. The input must be in the form of an FQDN (fully qualified domain name). The FQDN used must clearly show as A record (ARR) on the IP address of the MTAs. The FQDN recorded and used in DNS must be specified in the SMTP dialog (envelope communication) for the HELO/EHLO command. The hostname must not contain the server's IP address (e.g. server-80-12-54-125.example.org).
- 2.12 The WHOIS data of the IP address or the associated FQDNs must clearly reference the certified mailer. Furthermore, the IP addresses and FQDN must contain contactable email addresses and general abuse email addresses that are easy to find in the WHOIS information (see also RFC 2142, RFC 3013 Section 2.5 and current guidelines/best practices for RIRs and registries).

- 2.13 The mailer must set up a separate abuse/complaint or feedback loop email address if necessary (user-definable ROLE account for the mailer that is responsible for delivering automated complaints or requests from ISPs or recipients as applicable) for the IP addresses used by it and must announce it to the CSA. The ability to handle ARFs and X-ARF is required (see RFC 5965)⁴. Furthermore, designated contacts with a telephone number and email address for complaints must be provided. The maximum response time for ISP requests is 24 hours for working days.
- 2.14 The mailer must have sole control of the outbound mail server.
- 2.15 The outbound email servers specified by the mailer may only be used for bulk mailings and/or automated delivery. Ideally, it must e.g., be possible to assign specific campaigns or mailings to certain dedicated systems.
- 2.16 The mailer must take email addresses from mailing lists, if, after sending to this address, the mailbox is identified as non-existent, at the latest, however, after three hard bounces.⁵
- The hard bounce rate per ISP may not exceed 1.0% in total. An exception to this is only possible for new customers if the permitted hard bounce rate is exceeded once.
- 2.17 An SPF FROM record must be entered in the MAIL FROM address specified in the SMTP communication between the email servers. This allows SPF systems at the recipient to perform an SPF test (SRS procedures must also be implemented by the mailer as necessary for this purpose). The SPF record must end with "~all" or "-all".
- 2.18 There must be an SPF HELO record for the FQDN of the outbound email server and this should end in "-all", equivalent to the recorded information from 2.11.
- 2.19 With regard to the MAIL FROM address specified in the envelope communication between email servers, an additional MX record, as required and potentially allocated with lowest priority, and an A record must exist for its domain name part, which both point to the outbound email server.
- 2.20 The DKIM process (domain keys identified mail)⁶ must be implemented at the latest following successful certification by the CSA for all servers/IP addresses to be certified. The domains used in the DKIM "d=" tag must point either to the certified mailer via the WHOIS record or to the customer concerned for the certified mailer. The signed headers must include at minimum the "From", X-CSA-Complaints and list-unsubscribe.
- 2.21 A list-unsubscribe header (see RFC 2369)⁷ must be inserted, whereby exclusive use of a mailto-link is not permitted under the scope of the CSA. The specified links must enable the recipient to unsubscribe via an easy single-click at least at list level. The mailer may send a confirmation

⁴ See <http://www.x-arf.org>

⁵ email server status codes beginning with five (5) must be classified as a "hard bounce". See, e.g. RFC 3463

⁶ See <http://www.dkim.org>

⁷ See also <http://en.wikipedia.org/wiki/VERP> and <http://www.list-unsubscribe.com/>

email to the user when successfully unsubscribed.

Exceptions to this mandatory requirement may be justified if, due to the service's design and the resulting delivery of automated emails, unsubscribing is not required or possible as previously stipulated. The Complaints office shall decide upon any such exception. In the event of an exception, a list help link (see RFC 2369)⁸ must be inserted into the header, whereby the exclusive use of a mailto link is not permitted under the scope of the CSA. The link must lead to a help or login page that explains to the recipient how he/she can unsubscribe from any further mailings or why this is not possible on legal grounds, specifying these reasons.

- 2.22 Until two weeks after successful certification at the latest, a mailer must add an "X-CSA-Complaints" header. The header has to be "X-CSA-Complaints: whitelist-complaints@eco.de". This has to be confirmed by sending a sample to samples@certifiedsenders.eu.
- 2.23 DKIM failure reporting by the recipient must be made possible by recording or expanding the appropriate DNS records. DKIM failure reports must be accepted by the certified mailer or its customer(s) (see RFC 6651).

SPF failure reporting (for SPF MFROM and SPF HELO) by the recipient must be made possible by recording or expanding the appropriate DNS records. SPF failure reports must be accepted by the certified mailer or its customer(s) (see RFC 6652).

3 Recommended Admission Criteria /Double OPT-IN

- 3.1 In principle, when obtaining user data via the Internet, it is recommended to use the double opt-in process (DOI). 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 mailer 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 DOI, 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. The confirmation email may not contain any advertising or other content. The CSA participants agree to only describe the procedures implemented by them as DOI if they comply with these requirements.
- 3.2 As soon as a newsletter e.g. is requested, providing information regarding the expected frequency of mailings is recommended if a frequency has been set or is planned.

⁸ See also <http://en.wikipedia.org/wiki/VERP> and <http://www.list-unsubscribe.com/>

- 3.3 As soon as a newsletter e.g. is requested, providing the sender email address is also recommended to enable recipients to record this in their address book.
- 3.4 It is advisable to provide date and IP for the newsletter request in the header of the email to increase the chances of the user remembering that he/she actually subscribed. In addition, the subscriber information in the form of text should also be recorded in the body/text section of the email. The registered email address as well as the subscription date and the webpage where the recipient subscribed should be contained here.
- 3.5 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.
- 3.6 The exclusive handling of mailing campaigns for new customers via non-whitelisted mail servers is recommended.
- 3.7 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.
- 3.8 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.
- 3.9 It is advisable to send newsletters via other IPs than transactional emails.
- 3.10 Implementing 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 mailer or its customer(s). Putting a reject-policy in place is recommended.
- 3.11 Emails to the recipient should be delivered via a TLS-secured connection, provided the recipient supports it, in accordance with current BSI (German Federal Office for Information Security) guidelines or higher.

4 Lawfulness

- 4.1 The mailer is responsible for the mailing being performed lawfully and, in particular, for the content of the sent emails not being contrary to legal rules and restrictions.
- 4.2 In addition, the mailer is responsible for ensuring compliance with other legal requirements for the lawful implementation of the criteria as laid down in this document, for example, consent to send the registered IP address in an additional header row with every email.

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 bulk mailer shall have the right of extraordinary termination. In the event of termination, any contributions paid shall be refunded on a pro rata basis.