Council E-mail Technische Richtlijnen

Final

Versie:	*Council E-mail Technische Richtlijnen*
Auteur:	*Council E-mail, commissie E-Mail Service Providers*
Datum:	*10 november 2015*
Status:	*versie 7 (final)*

1 Algemeen

a. Deze Richtlijnen zijn bedoeld voor leden van de DDMA die een eigen platform bezitten en beschikbaar stellen aan derden voor het verzenden van ongevraagde reclame via e-mail. Er is sprake van ongevraagde reclame omdat het verzendmoment bepaald wordt door de verzender. De ontvanger heeft uiteraard wel toestemming gegeven om per e-mail reclame te ontvangen van de verzender of er bestaat een actieve klantrelatie op basis waarvan de verzender de ontvanger mag mailen.

b. Middels het lidmaatschap van de DDMA zijn deze leden gebonden de Code Reclame via E-mail te respecteren. De Richtlijnen zoals beschreven in dit document dienen als aanvulling op de Code Reclame via E-mail en bieden adverteerders en bestandseigenaren de garantie dat de geboden faciliteiten technisch juist ingeregeld zijn.

c. Inwerkingtreding: Deze Council E-mail Technische Richtlijnen zijn unaniem goedgekeurd door de Commissie E-mail Service Providers van de Council E-mail op <datum> en gaan in op <datum>.

d. De Richtlijn biedt een best practice en is een vrijwillig te implementeren instrument, waarmee platforms een universele technische standaard in e-mailverzending kunnen implementeren. Daarmee is echter niet gezegd dat er ook nog andere mogelijkheden zijn om daaraan te voldoen. Ondertekenaars van het ESP convenant van de Commissie E-mail Service Providers committeren zich aan het naleven van deze technische Richtlijnen.

e. Deze Richtlijnen gelden voor ondertekenaars van het ESP Convenant, bij verzending van commerciële, ideële of charitatieve boodschappen via e-mail door organisaties aan organisaties of particulieren.

f. Geldigheid: Deze richtlijnen zullen indien nodig of gewenst worden aangepast en geactualiseerd. De Commissie E-mail Service Providers initieert dit, de leden van deze commissie (de ESP's) kunnen hiervoor input leveren.

g. Artikelen in dit document zijn verplicht voor ondertekenaars van het ESP Convenant, tenzij de toevoeging **[AANBEVELING]** in het artikel is opgenomen.

2 Permissie en gegevensbeheer

AANMELDING/OPT-IN

a. De ESP dient technische mogelijkheden te bieden aan haar klanten waarmee op basis van double opt-in e-mailadressen verzameld kunnen worden.

b. In verband met de juridische bewijslast dienen gegevens betreffende waar, wanneer, de gehanteerde opt-in tekst, het geldende privacy statement en via welke methode toestemming (en bevestiging) van de geadresseerde is verkregen om e-mail te versturen (opt-in data), bewaard te worden. De vastgelegde informatie kan bijvoorbeeld bestaan uit: webformulier-url, datum van formulier invullen, IP van bezoeker, verzendmoment bevestigingsmail, datum van bevestiging (clicks), IP van ontvanger bevestigingsmail.

c. De ESP dient technische mogelijkheid te bieden aan haar klanten om deze gegevens gedurende de door regelgever opgelegde periode te bewaren. Deze periode is 60 maanden gerekend vanaf het moment dat de toestemming zijn geldigheid heeft verloren.

AFMELDING/OPT-OUT

d. De e-mail dient bij een actieve opt-in voorzien te worden van een list-unsubscribe header (RFC2369).

e. Afmeldprocedures die vanuit de ESP geboden worden dienen onbelemmerd te zijn. Zo zijn afmeldprocedures bij voorkeur pre-filled en niet voorzien van een wachtwoord.

BEHEER

f. De ESP dient faciliteiten te bieden waarmee het mogelijk is om non-response (inactieve ontvangers) op te schonen.

BOUNCES

g. Bounces moeten correct ontvangen, afgehandeld en verwerkt worden, zie ook RFC3463, RFC5321 en RFC5322.

h. De verzendende server dient de responses van de ontvangende server correct en volgens het SMTP protocol te interpreteren. Het gaat hier in het bijzonder om het correct reageren op tijdelijke fouten (4xx) of permanente fouten (5xx), zie RFC3463.

COMPLAINTS

i. Zorg voor een werkend postmaster@.. mail-adres op het domein van de verzender (sender-from en envelope-sender), zie ook RFC5321.

j. Zorg voor een werkend abuse@.. mail-adres op het domein van de verzender (sender-from en envelope-sender) en meld het domein van de verzender aan bij abuse.net **[AANBEVELING]**.

k. Maak gebruik van de feedback-loops van ISP's/MSP's **[AANBEVELING]**.

l. Lees en beantwoord altijd e-mail/berichten welke u ontvangt van maintainers van spamlists, system-operators, mail administrators, etc. **[AANBEVELING]**.

BEVEILIGING

m. Implementeer bestands- en gegevensuitwisseling via FTPS/SFTP en HTTPS **[AANBEVELING]**.

n. Voorkom zichtbare, tot de persoon herleidbare gegevens in de procedure-urls. Gebruik versleutelde waarden.

3 Content en codering

HEADERS

a. De 'From' header en de 'ReplyTo' header dienen bestaande, werkende e-mailadressen te bevatten.

b. De 'To' header dient tenminste het e-mailadres van de geadresseerde te bevatten, optioneel kan de naam van de geadresseerde worden toegevoegd (zie RFC2822).

CODERING

c. De e-mail bevat altijd een tekstvariant, dus wordt in multipart of plain-text variant verstuurd, tenzij de geadresseerde expliciet een voorkeur heeft aangegeven.

d. Pas geen onnodige encodering toe op de From en Subject header.

CONTENT

e. De ESP biedt de verzender functionaliteit voor het uitvoeren van automatische spamtests **[AANBEVELING]**.

f. Grafische content in de vorm van plaatjes (zoals bitmaps/gif/jpg) dienen online of inline te worden aangeboden, en niet als attachment met de mail zelf te worden verzonden.

4 Infrastructuur en verzending

VERZENDENDE MAILSERVERS

a. Voor verzendende mailservers dienen correcte en publiekelijk toegankelijke DNS- en reverse DNS records aanwezig te zijn. Het reverse DNS record verwijst naar de hostname.

b. De ESP dient consistent te zijn in het gebruik van IP-adressen en domeinnamen; maak zoveel mogelijk gebruik van een beperkt aantal aansluitende/congruente IP-adressen en/of IP-ranges. Geen snow-shoeing of wisselende IP-adressen.

c. Indien er gebruik gemaakt wordt van een eigen IP reeks bij RIPE dient de eigenaar van het IP adres eenvoudig herleidbaar zijn.

d. Verzendende mailservers dienen tijdens aflevering de fully-qualified hostname te gebruiken als HELO-naam.

e. Verzendende mailservers dienen afdoende beveiligd te zijn tegen misbruik, met nadruk op ongewenste relaying.

AUTHENTICATIE

f. Voor verzendende mailservers dienen correcte en publiekelijk toegankelijke Sender Policy Framework (SPF) records aanwezig te zijn t.b.v. afzenderverificatie (~all en –all zijn toegestaan). Vermeldt alle IP adressen, waarvandaan legitieme e-mail kan worden gestuurd namens een domein, in het DNS record voor dat betreffende domein. Gebruik DNS records van het type TXT voor de registratie van de SPF gegevens.

g. Maak gebruik van DomainKeys Indentified Mail (DKIM) om de authenticiteit van de e-mail tijdens ontvangst te kunnen verifiëren. Tevens kan gebruik van DKIM op een positieve manier bijdragen aan uw reputatie als verzender. DKIM is een methode om te verifiëren of een afzender authentiek is, een DKIM bestaat uit een versleutelde digitale handtekening welke door de ISP gelezen wordt om de authenticiteit van de e-mail te verifiëren **[AANBEVELING]**.

h. Stimuleer als ESP dat er met DMARC compliant verzenddomeinen wordt verzonden. Met Domain-based Message Authentication, Reporting and Conformance (DMARC) is het mogelijk om aan te geven hoe ontvangende mailservers (o.a. ISP's) om moeten gaan met: ongeauthenticeerde e-mail en/of e-mail waarbij de authenticatie mechanismes (SPF/DKIM) tussen verzending door de ESP en aflevering bij de ISP niet meer gevalideerd kunnen worden. Het criteria is wel dat de e-mail claimt afkomstig te zijn van het gebruikte afzenddomein wat door de ESP gebruikt wordt waarop het DMARC DNS record is geïmplementeerd.

   Met behulp van DMARC is het mogelijk om ongewenst gebruik van het e-mail afzenddomein door derden te verhinderen, de ontvangende ISP moet echter wel DMARC ondersteunen. Tevens geeft DMARC door middel van rapportages inzage in hoe ontvangende partijen om gaan met de ontvangen e-mail. **[AANBEVELING]**.

VERZENDING

i. Bij de verzending dient rekening te worden gehouden met de beperkingen van het netwerk en de eventuele afleverpolicies van de eigenaar/beheerder van de ontvangende mail servers (ISP's/MSP's).

j. De verzendende server dient correct te reageren op *transient errors* (bijv. service unavailable, rate limits, blacklisted).

k. Als verzending naar een bepaald adres tijdelijk mislukt, dan dient de frequentie van de retries (verzendpogingen) beperkt te zijn. Minimale interval van tien minuten gedurende maximaal drie dagen.

l. De ESP dient zorg te dragen voor goede, proactieve monitoring van de status op eventuele blacklists en van de reputatie als verzender **[AANBEVELING]**.