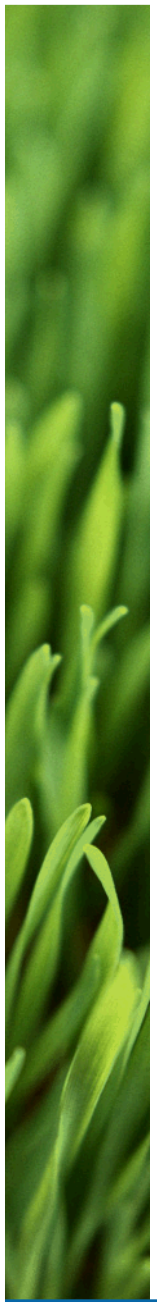
De beveiliging van persoonsgegevens

Kluwer
a Wolters Kluwer business

NATIONAAL PRIVACY CONGRES 20/11 2009

Gerrit-Jan Zwenne



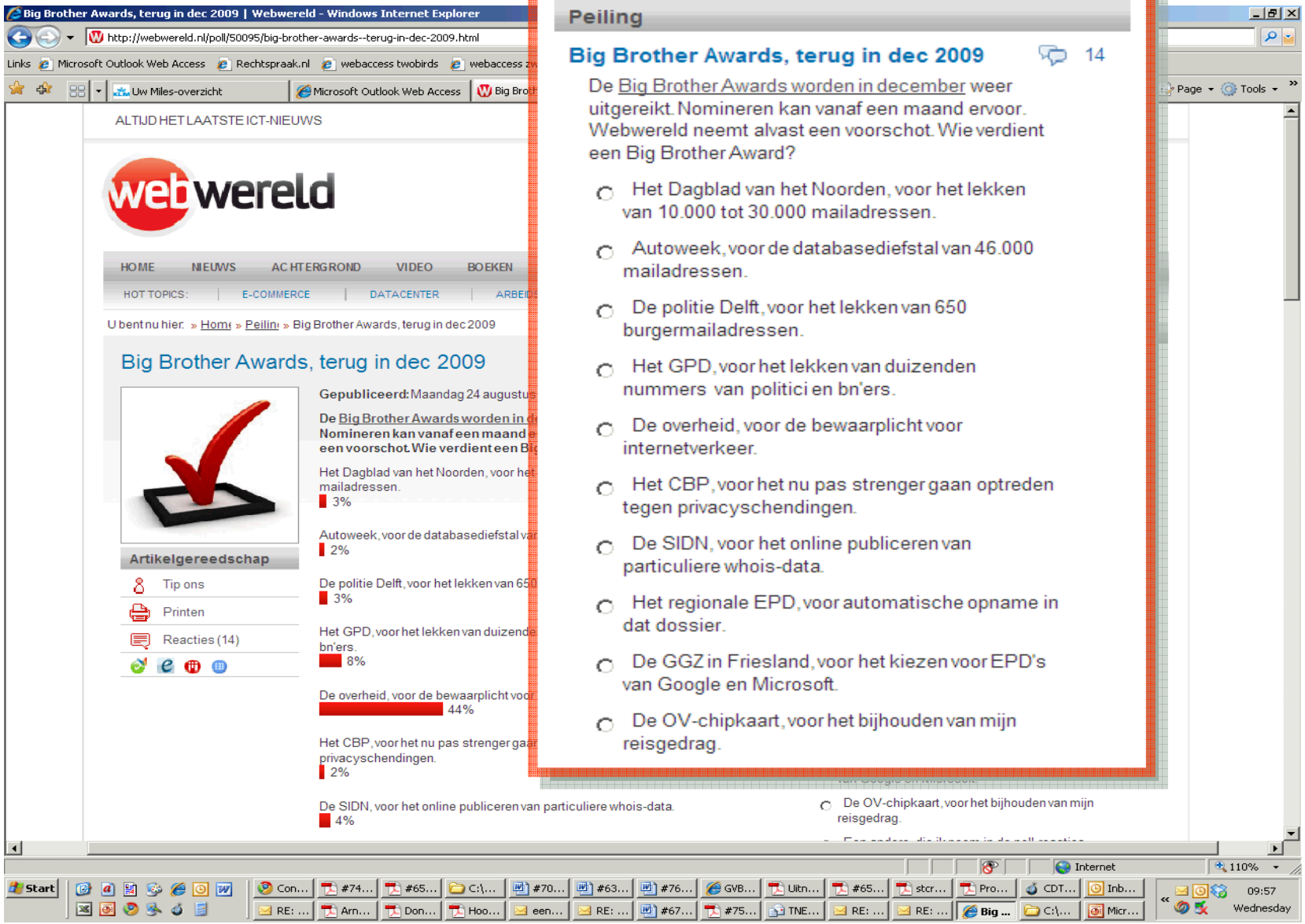
'Webshops slecht beveiligd'

De Pers nl

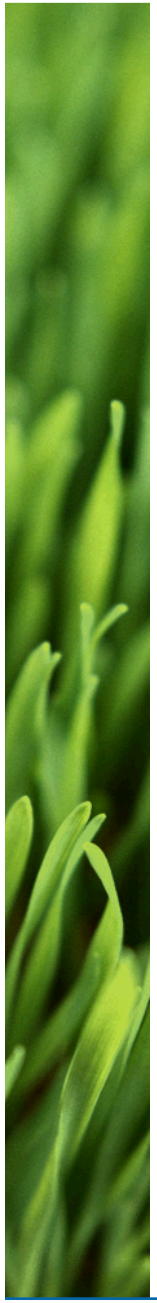
Het overgrote deel van de webwinkels waar via iDEAL kan worden betaald, is onvoldoende beveiligd. Dat blijkt uit onderzoek van internetbeveiliger Networking4all.

[18-11-2009] Van de ruim 13.000 webwinkels in Nederland, heeft volgens de internetbeveiliger 12 procent de beveiliging op orde. De uitkomsten van het onderzoek zijn woensdag door het bedrijf gepubliceerd. Volgens het internetbedrijf groeit het aantal niet goed beveiligde sites sneller dan het aantal dat de zaakjes wel op orde heeft.

Networking4all wijst er op dat webshops volgens de Wet bescherming persoonsgegevens verplicht zijn het verzenden van persoonsgegevens te beveiligen. Het College bescherming Persoonsgegevens adviseert webwinkeliers gebruik te maken van zogeheten SSL-certificaten.


Big Brother Awards, terug in dec 2009 | Webwereld - Windows Internet Explorer
http://webwereld.nl/poll/50095/big-brother-awards--terug-in-dec-2009.html
ALTIJD HET LAATSTE ICT-NIEUWS
webwereld
HOME NIEUWS ACHTERGROND VIDEO BOEKEN
HOT TOPICS: E-COMMERCE DATACENTER
U bent nu hier: » Home » Peilin » Big Brother Awards, terug in dec 2009
Big Brother Awards, terug in dec 2009
Gepubliceerd: Maandag 24 augustus
De Big Brother Awards worden in d
Nomineren kan vanaf een maand e
een voorschot. Wie verdient een Bi
Het Dagblad van het Noorden, voor het
mailadressen.
3%
Autoweek, voor de databasediefstal var
2%
De politie Delft, voor het lekken van 650
3%
Het GPD, voor het lekken van duizende
bn'ers.
8%
De overheid, voor de bewaarplicht voor
44%
Het CBP, voor het nu pas strenger gaar
privacyschendingen.
2%
De SIDN, voor het online publiceren van particuliere whois-data.
4%
Artikelgereedschap
Tip ons
Printen
Reacties (14)
Peiling
Big Brother Awards, terug in dec 2009
14
De Big Brother Awards worden in december weer uitgereikt. Nomineren kan vanaf een maand ervoor. Webwereld neemt alvast een voorschot. Wie verdient een Big Brother Award?
Het Dagblad van het Noorden, voor het lekken van 10.000 tot 30.000 mailadressen.
Autoweek, voor de databasediefstal van 46.000 mailadressen.
De politie Delft, voor het lekken van 650 burgermailadressen.
Het GPD, voor het lekken van duizenden nummers van politici en bn'ers.
De overheid, voor de bewaarplicht voor internetverkeer.
Het CBP, voor het nu pas strenger gaan optreden tegen privacyschendingen.
De SIDN, voor het online publiceren van particuliere whois-data.
Het regionale EPD, voor automatische opname in dat dossier.
De GGZ in Friesland, voor het kiezen voor EPD's van Google en Microsoft.
De OV-chipkaart, voor het bijhouden van mijn reisgedrag.
De OV-chipkaart, voor het bijhouden van mijn reisgedrag.
Start
09:57
Wednesday

BIRD & BIRD



The Register

Data protection watchdog distributes email mailing list

29-10-2004 The Dutch Data Protection Authority (Dutch DPA), which supervises the compliance with acts that regulate the use of personal data, was rather red-faced this week when it sent out a newsletter with all of the recipients in the Cc: field instead of the Bcc: field.

DPA's news letter goes out to 4000 subscribers. The DPA, which supervises the compliance with the Dutch Personal Data Protection Act was lucky that 'only' a thousand subscribers received the letter, but it managed to make the mistake twice. In a message it apologised for sending the first letter, again putting all recipients to the Cc list, so a second apology had to be sent.

<gert.wabeke@kpn.com>, <twagemans@ebay.com>, <j.wester@minez.nl>, <m.wiegel@nctb.nl>, <leon.de.wit@nl.pwc.com>, <a.p.h.g.van.zantvoort@minjus.nl>, <hz@kahuna.nl>, <gerrit-jan.zwenne@twobirds.com>, <righard.zwienenberg@norman.no>
Cc: "Dries, Hein" <H.Dries@opta.nl>, "Man, Mei Po" <M.Man@opta.nl>
Conversation: Consultatiedocument voorgenomen beleidsregels basismaatregel ogv art. 11.3 Tw
Subject: Consultatiedocument voorgenomen beleidsregels basismaatregel ogv art. 11.3 Tw

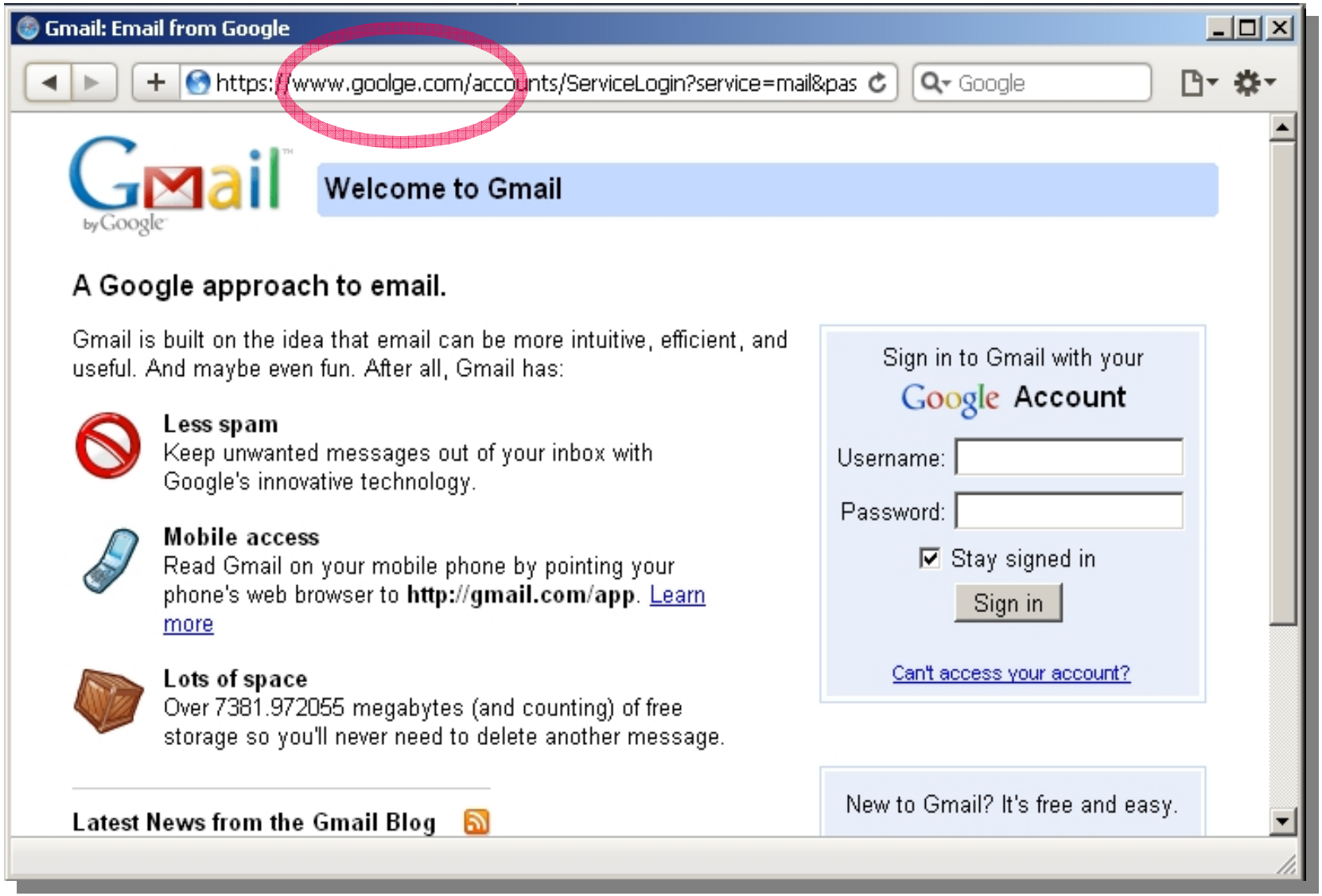
Geachte heer/mevrouw,

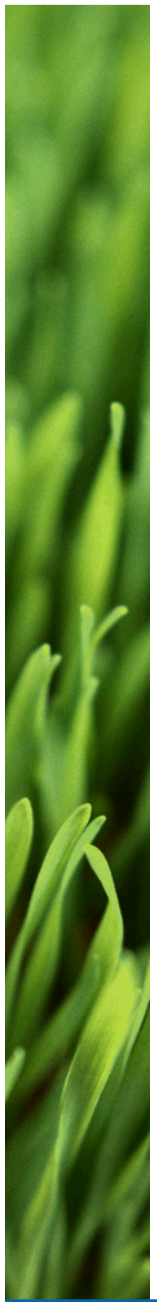
Hierbij ontvangt u het Consultatiedocument beleidsregels basismaatregelen op grond van artikel 11.3 van Telecomwet.

Voor verdere informatie verwijs ik u naar de bijlagen die in deze email zijn bijgevoegd.

Met vriendelijke groet,

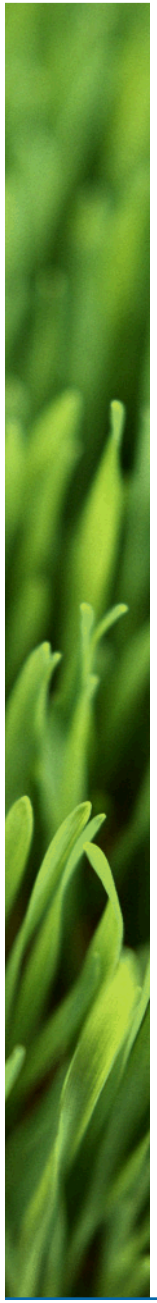
mw. **[XXXX] [XXXXXXX]**
Secretariaat IPB
Opta Onafhankelijke Post en
E-Mail: **[x.xxxx]**@opta.nl
Tel.: + 31 (0)70 - 3159232
Fax: + 31 (0)70 - 3153501
P.O. Box 90420; NL-2509 LK
H Muzenstraat 41; NL-2511


Gmail: Email from Google
https://www.goolge.com/accounts/ServiceLogin?service=mail&pas
Google
Gmail by Google
Welcome to Gmail
A Google approach to email.
Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.
Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com/app. Learn more
Lots of space
Over 7381.972055 megabytes (and counting) of free storage so you'll never need to delete another message.
Latest News from the Gmail Blog
Sign in to Gmail with your Google Account
Username:
Password:
Stay signed in
Sign in
Can't access your account?
New to Gmail? It's free and easy.



beveiligingsplichten

art. 13 Wbp	art. 11.3 Tw	art. 9c WVIB	art. 7 WJSG	
NEN 7510	art. 13.5 Tw	art. 3d Kadasterwet	art. 4 Wet pol.gegevens	ISO 15408
art. 7 BBGAT	art. 7:453 BW	art. 33 BGBSNiZ	art. 2:5 Awb	



lex generalis

- passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking
- maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen
- de maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen

vage normen…

art. 13 Wbp

achtergrondstudie

- exclusiviteit, integriteit en continuiteit
- vier risicoklassen
- praktisch
- wat gedateerd
- nieuw! richtsnoeren beveiliging

"inwerkingtreding" in Q1 2010...

A&V 23
april 2001

BIRD & BIRD

passende maatregelen

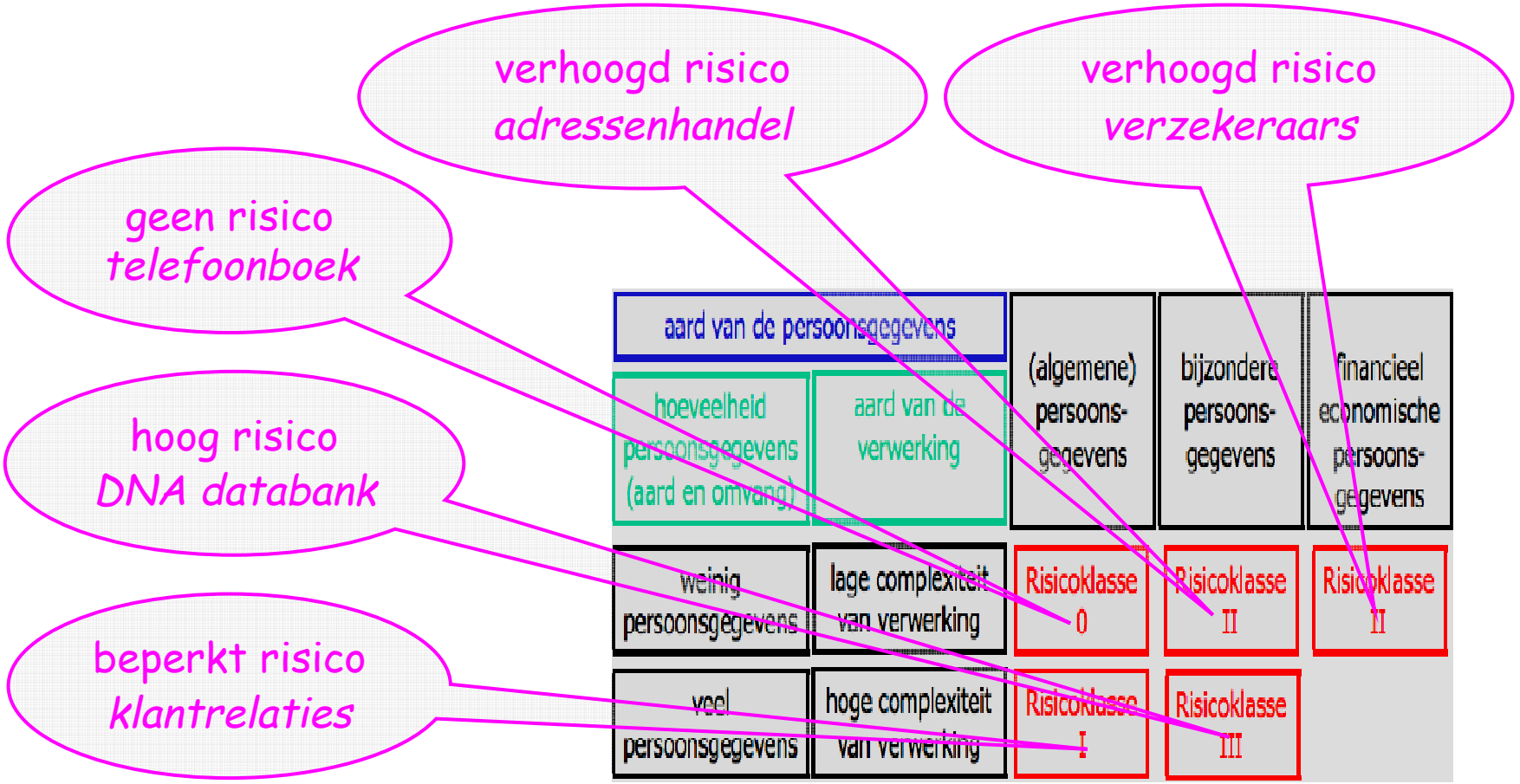
technisch
- toegangscontrole
- logfiles
- usb-sticks
- passwords
- backups
- enz.

organisatorisch
- verantwoordelijkheden
- bevoegdheden
- instructies
- trainingen
- beveiligingsplan
- enz.

passendheid
- stand v/d techniek
- kosten
- risico's

- *soort verwerking*
- *soort gegevens*
- *hoeveelheid cq. aantal betrokkenen*

risicoanalyse

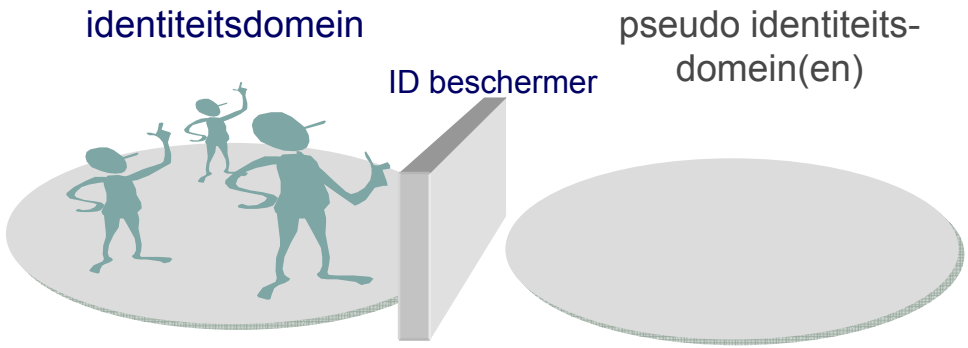


privacy enhancing technologies

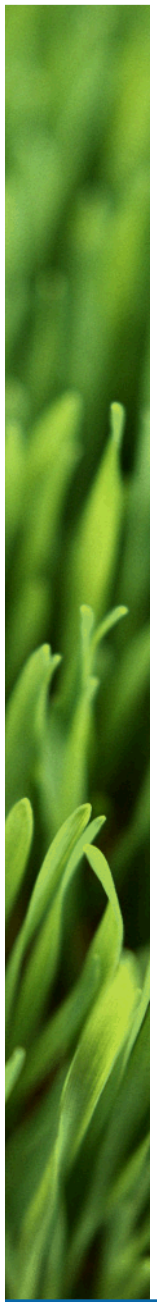
voorkomen onnodige verzameling en verdere verwerking van persoonsgegevens

pseudo-identiteit

- anonimity
- pseudonimity
- unlinkability
- unobservability



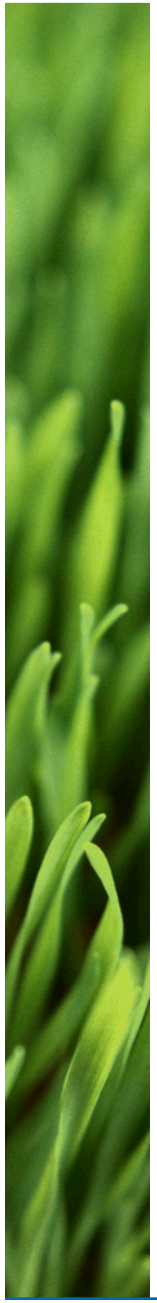
ISO 15408



‘Y vs Finland’

- *applicant [..] was unable to prove [..] that a casual connection between the deficiencies in the access security rules and the dissemination of information about her medical condition*
- *the mere fact that domestic legislation provided the applicant with the opportunity to claim compensation for damages caused by alleged unlawful disclosure of personal data was not sufficient to protect her private life*

EHRM 17 juli 2008
20511/03



‘anti-retrovirale middelen’

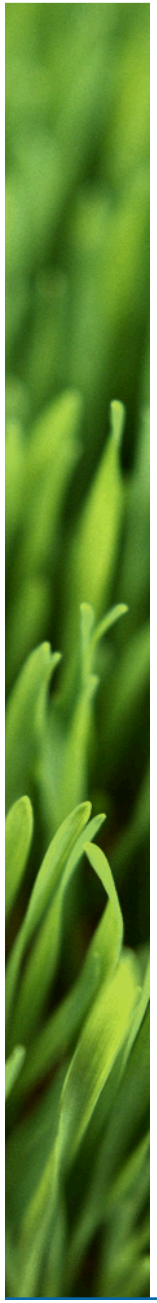
- beveiligingsplicht betreft ook mailing naar gebruikers van anti-retrovirale middelen

juist!

dus…

- ‘*persoonlijk*’ of ‘*vertrouwelijk*’ bij de adressering vermelden

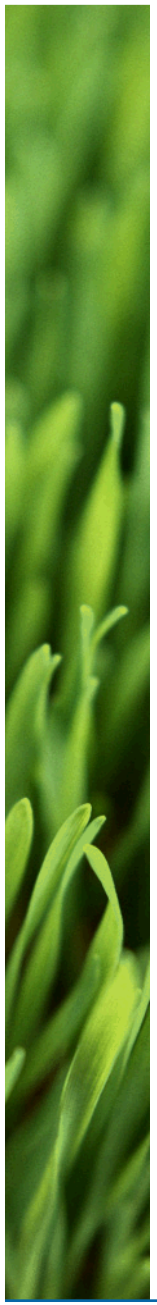
CBP 20 december 2004 z2004-0546



zorginformatiebeveiligingsnorm

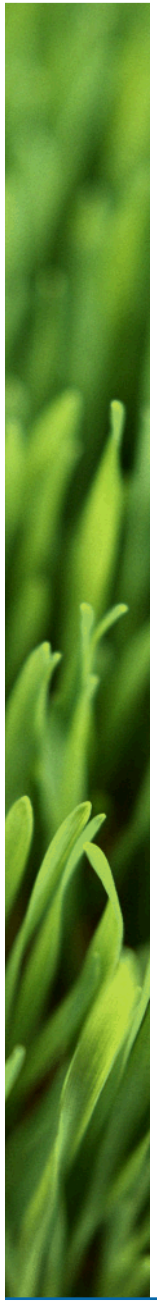
- NEN 7510 is gezaghebbende sectorale uitwerking van beveiligingsplicht in de zorg
- ijkpunten
  - organisatie (bestuurlijke verankering)
  - externe partijen (toegang)
  - beveiligingseisen t.a.v. personeel
  - toegangsbeveiliging (identificatie en authenticatie)
  - naleving wetgeving (compliance)
  - beveiligingsincidenten

CBP 20 december 2004 z2004-0546



LoD MC Lelystad e.a.

- uitvoeren risico-analyse informatiebeveiliging
- rapportage risico-analyse informatiebeveiliging
- opstellen functieprofiel en benoemen informatiebeveiligingsfunctionaris
- aanwijzen van portefeuillehouder informatiebeveiliging in Raad van Bestuur



outsourcing

bewerker

- geheimhoudingsplicht
- beveiligingsplicht

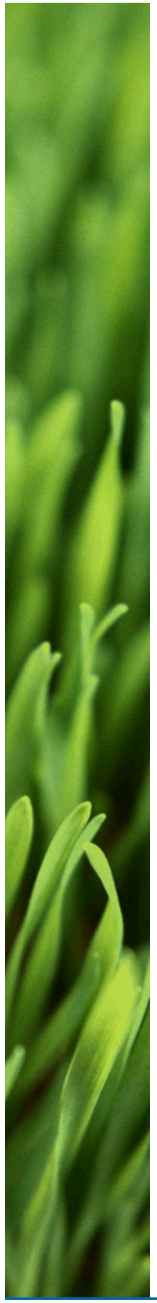
verantwoordelijke

- zorgplicht m.b.t. technische en organisatorische beveiligings-maatregelen

schriftelijke overeenkomst

1. Bewerker verwerkt gegevens ten behoeve van Verantwoordelijke, overeenkomstig diens instructies en onder diens verantwoordelijkheid. De verwerking vindt plaats op de wijze als is vastgelegd in bijlage 1.
2. Naast de verplichting van Bewerker om de instructies van de Verantwoordelijke te volgen, dient hij ook zorg te dragen voor…

art. 12 t/m 14 Wbp

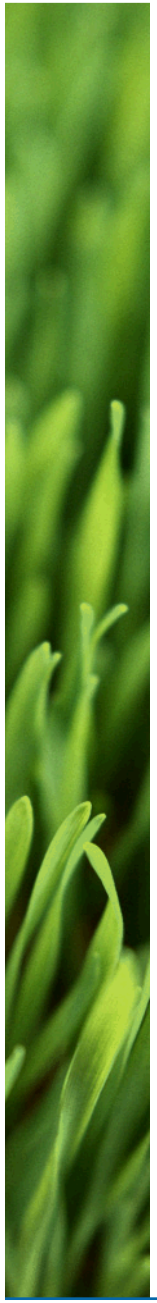


beveiligingsplicht isp's en telco's

- passende technische en organisatorische maatregelen t.b.v. beveiliging en veiligheid netwerken en diensten
- garanderen, rekening houdend met stand van techniek en kosten van tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot de risico's

vage normen..!

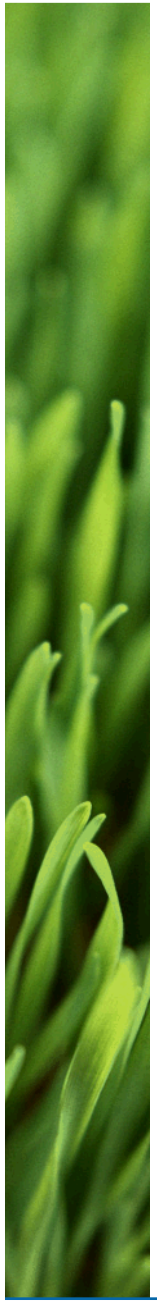
art. 11.3 -1 Tw



informatieplicht isp’s

- bijzondere risico's voor doorbreking van veiligheid of beveiliging van netwerk of aangeboden telecomdienst
- middelen waarmee deze risico's worden tegengegaan
- voor zover het andere maatregelen betreft dan die welke de aanbieder o.g.v. eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten

art. 11.3 -2 Tw



beleidsregels informatieplicht

veiligheidsrisico's

- spam
- botnets en zombies
- phishing
- spyware
- trojans
- WIFI-routers
- identity theft
- ongewenste websites
- enz

middelen

- spamfilters
- virus scanners
- firewall
- updates
- enz.

criteria

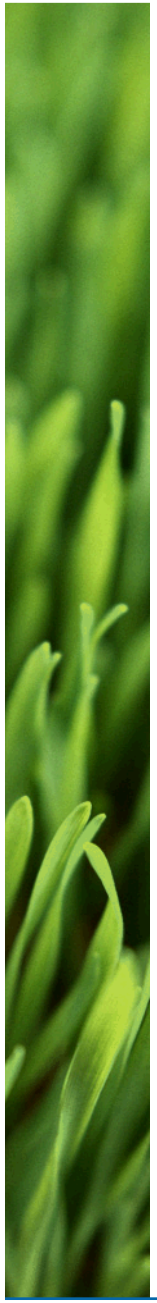
- duidelijk
- volledig
- actueel
- relevant

art. 11.3 -2 Tw

meldplicht beveiligingsinbreuken

- verplichting voor telco of ISP om OPTA ‘zonder onnodige vertraging’ melding te doen van beveiligingsinbreuken
- verplichting om aan abonnees of individuen onverwijld melding te doen als de inbreuk ‘waarschijnlijk ongunstige gevolgen’ heeft voor hun privacy
- maar niet als (volgens OPTA) gepaste technische beveiligingsmaatregelen zijn genomen

art. 4 rl. 2002/58



RICHTLIJN 2002/58/EG VAN HET EUROPEES PARLEMENT EN DE RAAD

van 12 juli 2002

betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)

Artikel 4 Veiligheid van de verwerking

3.In geval van een inbreuk in verband met persoonsgegevens stelt de aanbieder van openbare elektronische-communicatiediensten de bevoegde nationale instantie zonder onnodige vertraging in kennis van de inbreuk in verband met persoonsgegevens.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens en persoonlijke levenssfeer van een abonnee of individu stelt de aanbieder ook de abonnee of de persoon in kwestie onverwijld van de inbreuk in kennis.

Inkennisstelling van een abonnee of individuele persoon van een inbreuk op persoonsgegevens is niet vereist wanneer de dienstaanbieder tot voldoening van de bevoegde instantie heeft aangetoond dat hij de gepaste technische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de veiligheidsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang tot deze gegevens heeft.

Onverminderd de verplichting van de aanbieder om de abonnees en de personen in kwestie in kennis te stellen, indien de aanbieder de abonnee of persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan de bevoegde nationale instantie hem, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

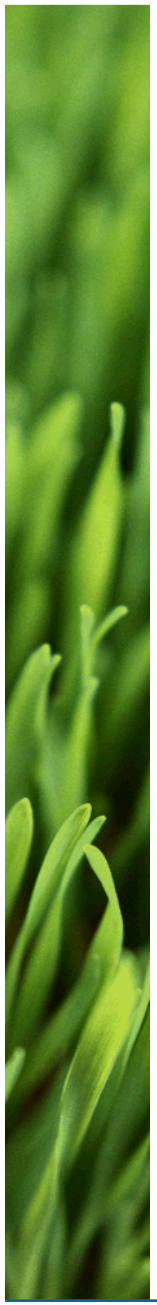
In de kennisgeving aan de abo[n]soonsgegevens, alsmede de contactpunten voor m[e]gevolgen van de inbreuk in verb[a]bovendien een omschrijvin[g] inbreuk in verband m[e]

straks ook diensten van de informatiemaatschappij?

4.Afhankelij[k]ale instanties richt[s]ng van de inbreuk in verband [m]elijke formaat, alsmede de manier waarop d[e] [h]un kennisgevingsverplichtingen overeenkomstig [l]ggen zij sancties op.

Aanbieders houden een zodanige inventaris bij van inbreuken op persoonsgegevens, o.m. de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, dat de bevoegde nationale instanties kunnen nagaan of de bepalingen van lid 3 worden nageleefd. De inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

Deze maatregelen, die niet-essentiële onderdelen van deze richtlijn beogen te wijzigen door haar aan te vullen, worden vastgesteld volgens de in artikel 20 bis, lid 2, bedoelde regelgevingsprocedure met toetsing.



vragen?

gerrit-jan.zwenne@twobirds.com