STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 8
14 januari 2009

Beleidsregels informatieplicht voor aanbieders over internetveiligheid (Artikel 11.3 tweede lid van de Telecommunicatiewet)

14 januari 2009

Inhoudsopgave

1 Inleiding

1.1 Algemeen

De Telecommunicatiewet geeft het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college) de bevoegdheid om op te treden tegen het niet-naleven van de informatieplicht over veiligheid en beveiliging van aangeboden diensten en netwerken.
Het college geeft in dit document invulling aan zijn handhavingsbeleid voor overtredingen van de informatieplicht en formuleert zijn specifieke bevoegdheid in dezen. Hierdoor wordt structuur gegeven aan de uitvoering van de handhaving van de informatieplicht en wordt willekeur voorkomen. Tevens geeft het college invulling aan zijn beleidsvrijheid ten aanzien van de keuze voor een bepaald handhavingsmiddel.

In elke individuele situatie wordt rekening gehouden met de specifieke omstandigheden van het betreffende geval. Een besluit om over te gaan tot handhaving en de keuze voor het handhavingsmiddel is immers altijd maatwerk.

Dit handhavingsbeleid wordt extern bekend gemaakt door plaatsing ervan in de Nederlandse Staatscourant en op de website van OPTA.[1]

1.2 Internetveiligheid

Internetveiligheid is een onderwerp dat een brede maatschappelijke belangstelling kent. Iedereen die zich regelmatig op internet begeeft, wordt geconfronteerd met aanzienlijke aantallen ongewenste e-mailberichten.[2] Vele Nederlanders zullen via het nieuws gehoord hebben over e-mails waarin argeloze PC-gebruikers wordt gevraagd hun inloggegevens voor elektronisch bankieren terug te sturen,[3] of over personen die ongemerkt PC's van anderen gebruiken voor criminele activiteiten.[4] Ouders zijn vaak bezorgd over hoe zij hun kinderen kunnen beschermen tegen pesten via internet, of tegen kwaadwillende personen die zich voordoen als iemand anders, of tegen het risico dat hun kinderen terechtkomen op een webpagina die niet voor kinderen is bestemd. Kortom, er is brede maatschappelijke aandacht voor de risico's die zijn verbonden aan het gebruik van internet en het is voor de leek – en vaak ook voor de meer ervaren internetgebruiker – niet altijd duidelijk wat deze risico's zijn en hoe deze tegengegaan kunnen worden.

---

1 Zie www.opta.nl.
2 In 2007 bestond naar schatting 90 tot 95 procent van het e-mailverkeer uit spam. Zie bijvoorbeeld http://www.nu.nl/news/1353927/50/'Slechts_1_op_20_e-mails_is_geen_spam'.html
3 Klanten van banken krijgen met regelmaat e-mailberichten waarin om hun creditcardgegevens wordt gevraagd. Zie bijvoorbeeld het bericht van 22 juli 2008 op http://www.zdnet.nl/smartbiz.cfm?id=88513. En in juni 2008 ontvingen houders van een Zonnet e-mail abonnement een bericht waarin hen werd gevraagd hun inloggegevens te verstrekken. De afzender van dit bericht deed zich voor als Zonnet. Zie http://www.websonic.nl/nieuws/062008/tele2_phishing_mail.php.
4 Zie bijvoorbeeld het bericht van 2 augustus 2008 op http://www.techzine.nl/nieuws/17269/19-jarige-hacker-opgepakt-vanwege-verkoop-botnet.html.

1.3 Wetgeving

De wetgever heeft in de Telecommunicatiewet (hierna: de Tw) meerdere bepalingen opgenomen die ertoe moeten leiden dat de veiligheid van internetgebruik toeneemt. Artikel 11.3 Tw is gericht op aanbieders van openbare elektronische diensten en netwerken en bestaat uit twee delen: het eerste lid betreft een verplichting aan netwerk- en dienstaanbieders (hierna: aanbieders) om hun diensten en netwerken te beveiligen (hierna: beveiligingsplicht) en het tweede lid betreft de verplichting aan aanbieders om hun abonnees voor te lichten over veiligheidsrisico's (hierna: informatieplicht). Tezamen worden deze verplichtingen vaak aangeduid als de zorgplicht. Het college heeft de taak toezicht te houden op de naleving van deze bepaling.

1.4 Internationale aandacht

Gezien het grote maatschappelijk belang en de omvang van de risico's van internetgebruik, geeft het college hoge prioriteit aan deze taak. Daarin staat het college niet alleen. Ook in Europees verband is er veel aandacht voor internetveiligheid. De Europese Commissie heeft diverse voorstellen gedaan om de internetveiligheid te vergroten. Ook ENISA,[5] het agentschap van de Europese Unie voor netwerk- en informatiebeveiliging, heeft onlangs een rapport[6] uitgebracht waarin aanbevelingen staan hoe lidstaten in de toekomst informatiebeveiliging zouden moeten nastreven. Eén van de aanbevelingen uit dit rapport is bijvoorbeeld de invoering van een wettelijke plicht om beveiligingsincidenten te melden aan een toezichthouder, onder welke plicht dus ook aanbieders van elektronische communicatiediensten en -netwerken zouden komen te vallen.

1.5 Rol van het college bij internetveiligheid

Het college is er zich terdege van bewust dat internetveiligheid afhankelijk is van veel meer partijen dan alleen de aanbieders van elektronische communicatiediensten en -netwerken: ook leveranciers van soft- en hardware, hosting aanbieders en eindgebruikers zijn verantwoordelijk voor veiligheid op het internet. Het artikel in de Tw heeft echter alleen betrekking op aanbieders van elektronische communicatiediensten en -netwerken en de bevoegdheid van het college gaat dus niet verder dan het toezicht op alleen deze partijen.

Het college heeft aan het begin van 2008[7] aangegeven drie speerpunten te zien op het gebied van de zorgplicht. Ten eerste de informatieplicht van aanbieders, met andere woorden, de voorlichting door ISP's van hun abonnees over veiligheidsrisico's. Ten tweede het ontwikkelen van een keurmerk door ISP's voor hun eigen branche. Met dit keurmerk voor ISP's zouden abonnees een weloverwogen keuze kunnen maken en zo hun eigen verantwoordelijkheid kunnen nemen bij internetveiligheid door die ISP te kiezen die een pakket biedt dat bij hun veiligheidsbehoefte en kennis aansluit. Ten derde de aanpak van het probleem van zombiecomputers, dat wil zeggen, PC's waarvan de besturing in handen is gevallen van personen die met deze PC's criminele activiteiten ontplooien. Het eerste speerpunt, de informatieplicht, staat centraal in deze beleidsregels.

1.6 Reacties op de consultatie van de voorgenomen beleidsregels

Op 22 september 2008 heeft het college zijn voorgenomen beleidsregels gepubliceerd. Er is daarop gereageerd door T-Mobile, Scarlet Telecom, en – door middel van een gezamenlijke reactie – door NLKabel, KPN, UPC, XS4ALL, Ziggo, bbned, BT, COLT, Online, Priority, Tele2 en Verizon Business.

Het college constateert dat alle respondenten, met uitzondering van T-Mobile, zich in hoofdlijnen in de voorgenomen beleidsregels kunnen vinden. Een ruime meerderheid van de aanbieders onderschrijft het belang van het verstrekken van adequate informatie aan abonnees over de risico's van internet-gebruik. De voorgestelde manier van handhaving door het college wordt in hoofdlijnen gesteund.

Het college heeft dankbaar gebruik gemaakt van de ontvangen reacties bij het vaststellen van de onderhavige beleidsregels. In een aparte bijlage[8] bij deze beleidsregels gaat het college in detail in op de ingebrachte op- en aanmerkingen, zodat de respondenten en andere geïnteresseerden kunnen nalezen hoe het college hiermee is omgegaan.

---

5 European Network and Information Security Agency.
6 Security Economics and the Internal Market, R. Anderson et al., februari 2008.
7 Tijdens de door ECP.nl georganiseerde bijeenkomst 'Derde Kamer Discussie Zorgplicht' van 13 februari 2008.
8 Deze bijlage is gepubliceerd op de website van OPTA.

1.7 Leeswijzer

Allereerst beschrijft het college in hoofdstuk 2 waarom hij beleidsregels noodzakelijk acht voor zijn toezicht op de informatieplicht. Vervolgens wordt in hoofdstuk 3 het juridisch kader beschreven. De beleidsregels beginnen in hoofdstuk 4 en 5, waar het college ingaat op wat er aan informatie dient te worden gegeven. In de woorden van artikel 11.3 Tw: welke bijzondere risico's minimaal zouden moeten worden genoemd en welke middelen in aanmerking komen om deze risico's tegen te gaan. Vervolgens beschrijft het college in hoofdstuk 6 en 7 voor wie de informatieplicht geldt en wie geïnformeerd dient te worden. Daarna geeft het college aan hoe en wanneer naar zijn mening een aanbieder de informatie dient te verstrekken (hoofdstuk 8) en tot slot beschrijft het college welke handhavingsmethoden hij zal gaan gebruiken (hoofdstuk 9).

2 Waarom beleidsregels voor de informatieplicht

2.1 Algemeen

Consumenten moeten zichzelf kunnen beschermen tegen de risico's van het gebruik van internet. Maar internet en internetdiensten kunnen complex van aard zijn. Niet iedere consument beschikt over voldoende deskundigheid of informatie om zich goed te kunnen wapenen tegen deze risico's. Daarom is het noodzakelijk dat zij goed geïnformeerd worden. Het college is daarom van mening dat het van groot belang is dat ISP's hun abonnees goed voorlichten over de veiligheidsrisico's die verbonden zijn aan internetgebruik. Niet voor niets heeft de wetgever met de informatieplicht uit artikel 11.3 tweede lid, Tw de verantwoordelijkheid bij de internetdienstaanbieder gelegd om de abonnee te informeren.[9]

2.2 Motivatie handhaving informatieplicht

Sommige aanbieders zullen ervoor kiezen om ruime invulling te geven aan de informatieplicht, omdat zij internetveiligheid als een van de manieren zien om zich te onderscheiden tegenover de concurrentie. Maar het college constateert dat er ook aanbieders kunnen zijn voor wie de informatieplicht minder prioriteit heeft. Immers, aanbieders vinden het niet altijd prettig om ook minder aantrekkelijke informatie over hun diensten te verschaffen, zoals een lijst van risico's die de abonnee loopt en de kosten en moeite die er bij komen om zich te beschermen tegen deze risico's. Daarbij komt dat de veiligheid rondom internet afhankelijk is van álle partijen. De investeringen of opofferingen die één aanbieder doet zullen niet volstaan om de veiligheid van zijn eigen abonnees te waarborgen, omdat de risico's afkomstig kunnen zijn vanuit het gehele internet, inclusief bijvoorbeeld concurrerende aanbieders en leveranciers van soft- en hardware. Met andere woorden, de oorzaak van de risico's ligt vaak buiten de reikwijdte van de aanbieder zelf. Een aanbieder zou daarom minder gemotiveerd kunnen zijn om aan de informatieplicht te voldoen. Alleen als iedereen zich inspant voor internetveiligheid zullen de risico's voor abonnees sterk afnemen. Een actieve rol van de toezichthouder is dan ook wenselijk om ervoor te zorgen dat alle aanbieders daadwerkelijk de informatieplicht nakomen.

Het college is daarom van oordeel dat het noodzakelijk is dat hij de informatieplicht uit artikel 11.3, tweede lid, Tw actief handhaaft. Om aanbieders duidelijkheid te geven hoe het college deze handhaving vorm gaat geven en welke criteria hij gebruikt om te beoordelen of een aanbieder aan de verplichting voldoet, maakt het college gebruik van onderhavige beleidsregels.

3 Juridisch kader

3.1 Algemeen

In de Privacy Richtlijn[10] (hierna: de Richtlijn) wordt gesteld dat geavanceerde digitale technologieën specifieke eisen stellen aan de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker. In de overwegingen bij deze Richtlijn wordt uitgelegd dat aanbieders van diensten de nodige maatregelen moeten treffen om de beveiliging van hun diensten te garanderen en dat zij de abonnees moeten informeren over eventuele bijzondere risico's inzake het doorbreken van de beveiliging van de dienst of het netwerk. Artikel 4 van de Richtlijn legt deze verplichting vast. De wetgever heeft dit artikel geïmplementeerd in artikel 11.3 van de Tw.

3.2 De Richtlijn

Artikel 4 van de Richtlijn luidt:

---

[9] Ook hier weer de constatering dat ook bijvoorbeeld leveranciers van software en hardware de consument zouden moeten voorlichten over risico's, maar daarover is (nog) geen verplichting opgenomen in de Telecommunicatiewet.

[10] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002, L 201/37.

Beveiliging

1. *De aanbieder van een openbare elektronische-communicatiedienst treft passende technische en organisatorische maatregelen om de veiligheid van zijn diensten te garanderen, indien nodig in overleg met de aanbieder van het openbare communicatienetwerk wat de veiligheid van het netwerk betreft. Die maatregelen waarborgen een beveiligingsniveau dat in verhouding staat tot het betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering ervan.*
2. *Indien een bijzonder risico bestaat van inbreuken op de beveiliging van het netwerk, stelt de aanbieder van een openbare elektronische-communicatiedienst de abonnees in kennis van dat risico en, indien het risico tot andere maatregelen noopt dan die waartoe de dienstenaanbieder verplicht is, van de eventuele middelen om dat risico tegen te gaan, met inbegrip van een indicatie van de verwachte kosten.*

3.3 De Telecommunicatiewet

Artikel 11.3, Tw luidt:

1. *De in artikel 11.2 bedoelde aanbieders[11] treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.*
2. *De in artikel 11.2 bedoelde aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over:*
   a. *bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;*
   b. *de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.*

3.4 Bevoegdheid

Op grond van artikel 15.1, Tw is het college aangewezen als toezichthouder op de naleving van het bepaalde bij of krachtens artikel 11.3, Tw.

4 Bijzondere risico's

4.1 Algemeen

In dit hoofdstuk wordt ingegaan op het begrip 'bijzondere risico's' uit de informatieplicht van artikel 11.3, Tw.

4.2 Te adresseren risico's

In de Richtlijn wordt in overweging 20 gesteld:[12]

'Het is bijzonder belangrijk voor abonnees en gebruikers van openbare elektronische communicatiediensten om door hun dienstaanbieder volledig op de hoogte te worden gebracht van bestaande veiligheidsrisico's die van dien aard zijn dat de dienstaanbieder deze zelf niet kan verhelpen.'

Het betreft hier veiligheidsrisico's die een inbreuk kunnen maken op de persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers. De desbetreffende aanbieders zijn niet gehouden de abonnees te informeren over elk beveiligingsrisico. Het gaat om bijzondere risico's en dan met name die risico's die een bijzonder verband hebben met de aard van het betrokken netwerk of de betrokken dienst.[13] Zo heeft het risico van ongewenst medegebruik van een draadloze internetverbinding door andere eindgebruikers dan de abonnee een bijzondere band met de dienst internettoegang en houdt dit risico geen verband met een e-maildienst. Een aanbieder van wie de dienstverlening beperkt is tot het verzorgen van een e-maildienst behoeft dus geen informatie te verschaffen over de beveiliging van draadloze routers.

---

[11] Bedoeld worden de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst.
[12] Overweging 20 bij de Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002, L 201/37.
[13] Kamerstukken II, 1996/97, 25 533, nr. 3, p. 119.

Het college acht het noodzakelijk dat de volgende risico's minimaal geadresseerd worden door de aanbieder van de betreffende dienst.

Risico	Technische term	Bijzondere band met de dienst
1. Het binnenkrijgen of (ongemerkt) versturen van grote hoeveelheden ongevraagde berichten).	spam	internettoegang, elektronische berichten
2. Het gekaapt worden van de eigen computer door een niet-geautoriseerde gebruiker	botnet, zombie	internettoegang
3. Het binnenkrijgen of (ongemerkt) versturen van berichten die tot doel hebben persoonlijke gegevens van abonnees te achterhalen, bijvoorbeeld bankgegevens, PINcode of inlognaam.	phishing	elektronische berichten
4. Het binnenkrijgen of (ongemerkt) versturen van software die bedoeld is om te spionneren op (internet)gedrag van abonnees.	spyware	internettoegang, elektronische berichten
5. Het binnenkrijgen of (ongemerkt) versturen van software die bedoeld is om de computerapparatuur van abonnees zodanig te verstoren dat gegevens verloren gaan of voor de buitenwereld openbaar worden.	trojans en overige malware	internettoegang, elektronische berichten
6. Het ongewenst medegebruik van de draadloze internetverbinding door andere eindgebruikers, waardoor mogelijk strafbare of anderszins ongewenste activiteiten over deze verbinding aan de betreffende abonnee zouden kunnen worden toegeschreven, of waardoor andere eindgebruikers mogelijk toegang krijgen tot de computer van de abonnee.	beveiliging draadloze router	internettoegang
7. Het gebruik door anderen van de eigen identiteit, door bijvoorbeeld bekend worden van wachtwoord, e-mailadres, naam- adres- woonplaats- of geboortedatum gegevens.	identiteitskaping	internettoegang, elektronische berichten
8. Het bereikbaar zijn van of (ongevraagd) geconfronteerd worden met ongewenste websites, zoals websites die niet geschikt zijn voor kinderen.	ongewenste websites	internettoegang

Bovenstaande tabel bevat slechts voorbeelden. De markt voor internetdiensten is dynamisch en daarom kan een tabel als deze nooit volledig zijn. Het college verwacht van aanbieders dat zij nieuwe risico's in hun informatievoorziening opnemen.

5 Middelen en indicatie van de verwachte kosten

5.1 Geen middelen in beleidsregel

In het vorige hoofdstuk is ingegaan op de bijzondere risico's waarover abonnees geïnformeerd dienen te worden door de aanbieders. Volgens de informatieplicht dient een aanbieder tevens de abonnees te informeren over de eventuele middelen waarmee de bijzondere risico's kunnen worden tegengegaan. Het college is van mening dat het niet wenselijk is om in beleidsregels vast te leggen welke informatie over middelen het college als afdoende oordeelt voor een aanbieder om aan de informatieplicht te voldoen. De aanbieder is het best in staat om de juiste middelen te benoemen en op de hoogte te zijn van de verwachte kosten om deze middelen in te zetten. Daarom laat het college deze keuze aan de aanbieder.

5.2 Mogelijke middelen

In het algemeen kan het college wel melden dat het naar zijn mening gaat om voorlichting over middelen zoals een firewall, een e-mailfilter, een virusscanner, het gebruik van legale software, het activeren van automatische updates van software en gepaste voorzichtigheid bij het openen van aangeboden bestanden. Bij zijn toezicht zal het college nagaan of de informatie daadwerkelijk beschrijft hoe deze middelen de betreffende bijzondere risico's kunnen verkleinen.

5.3 Toezicht

Het college zal bij zijn toezicht van geval tot geval beoordelen of de verstrekte informatie tegemoet komt aan de eisen gesteld in het wetsartikel.

6. Aanbieders

6.1 Dienstaanbieders

Het college wil de markt duidelijk maken op welke aanbieders hij zijn focus zal leggen bij het toezicht op de naleving van de informatieplicht. Artikel 11.3, Tw spreekt over zowel aanbieders van openbare elektronische communicatiediensten als over aanbieders van openbare elektronische communicatienetwerken. De Richtlijn daarentegen legt uitsluitend een verplichting op aan aanbieders van openbare

elektronische communicatiediensten. De reden voor dit verschil ligt in de constatering van de wetgever dat een dienstaanbieder voor de veiligheid en de beveiliging van zijn dienst mede afhankelijk is van de inspanningen van de netwerkaanbieder en dat deze laatste daarmee dus eveneens verantwoordelijk is voor de veiligheid en de beveiliging van de aangeboden diensten en netwerken.[14] Omdat deze dienstaanbieders, in tegenstelling tot de netwerkaanbieders, een direct klantcontact hebben, zal het college zich bij het toezicht op de naleving concentreren op de dienstaanbieders.

6.2 Internetdiensten

Overweging 6 van de Richtlijn stelt het volgende:

Het internet vervangt traditionele marktstructuren door te voorzien in een gemeenschappelijke, wereldwijde infrastructuur voor de levering van een breed scala van elektronische-communicatiediensten. Algemeen beschikbare elektronische-communicatiediensten via het internet bieden de gebruikers nieuwe mogelijkheden, maar houden ook nieuwe gevaren in voor de bescherming van hun persoonsgegevens en persoonlijke levenssfeer.

Ook het college is van mening dat de grootste veiligheids- en beveiligingsrisico's bij abonnees zich voordoen bij diensten die te maken hebben met het internet. Door de technische complexiteit van die diensten lopen de persoonsgegevens en de persoonlijke levenssfeer van abonnees meer gevaar dan bijvoorbeeld bij klassieke vaste of mobiele telefoondiensten. Daarom zal het college zich bij het toezicht concentreren op aanbieders van diensten die te maken hebben met internet en niet op andere aanbieders van openbare elektronische communicatiediensten en -netwerken, zoals klassieke telefoonaanbieders. Hierbij wordt geen onderscheid gemaakt tussen vast en mobiel internet.

6.3 Aanbieders openbare elektronische communicatiediensten

Het is verder van belang om aandacht te schenken aan het onderscheid tussen aanbieders van openbare elektronische communicatiediensten en aanbieders van diensten van de informatiemaatschappij.[15] In die laatste categorie valt bijvoorbeeld de dienst elektronisch bankieren. Aanbieders van openbare elektronische communicatiediensten zijn op grond van artikel 11.3, tweede lid, Tw, uitsluitend verantwoordelijk voor generieke informatievoorziening over veiligheid die te maken heeft met het gebruik van internet, maar zijn niet verantwoordelijk voor gerichte informatievoorziening bij specifieke risico's voor specifieke diensten van de informatiemaatschappij. Bij het in Tabel 1 genoemde risico van phishing bijvoorbeeld, ziet het college er op toe dat aanbieders van internettoegang hun abonnees hierover generiek informeren, maar het college is van mening dat de verantwoordelijkheid voor het informeren over specifieke phishing acties niet bij de aanbieder van internettoegang ligt, maar bij de aanbieder van de dienst elektronisch bankieren.

7 Abonnees

De abonnees van een openbare elektronische-communicatiedienst kunnen zowel natuurlijke als rechtspersonen zijn.[16] Dat betekent dat zowel abonnees uit de zakelijke markt als uit de consumentenmarkt geïnformeerd dienen te worden door de aanbieders. Het college acht het aannemelijk dat bij grootzakelijke abonnees voldoende kennis over veiligheid en beveiliging aanwezig is. Daarom legt het college de focus op abonnees uit de consumentenmarkt en het midden- en kleinbedrijf. Dat neemt niet weg dat het college, wanneer daar aanleiding toe is, ook handhavend zal optreden tegen een aanbieder die niet voldoende voorlichting geeft aan grootzakelijke abonnees.

8 De wijze van informatieverstrekking

8.1 Algemeen

In dit hoofdstuk licht het college toe welke criteria hij hanteert voor het beoordelen van de manier waarop de informatie door de aanbieder wordt verstrekt aan zijn abonnees. Zo is het college van mening dat minimaal alle in hoofdstuk 4 genoemde bijzondere risico's bij de informatieverstrekking expliciet aan de abonnee uitgelegd dienen te worden. Verder zal het college er op toezien dat voor elk

[14] Kamerstukken II 1996/1997, 25 533, nr. 3, p.119.
[15] Een dienst van de informatiemaatschappij is elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn (artikel 3:15d lid 3 BW).
[16] Artikel 1.1 onder p, van de Tw.

van deze risico's de middelen aan de orde komen, met daarbij een indicatie van de verwachte kosten.[17]

8.2 Voorwaarden informatieverstrekking

Het college is van mening dat een aanbieder aan de gestelde informatieplicht voldoet indien de informatieverstrekking op een duidelijke en ondubbelzinnige manier plaatsvindt. Een vereiste is dat de informatie actueel en relevant is.

8.3 Toegankelijkheid informatieverstrekking

Verder is het college van mening dat de betreffende informatie gemakkelijk en permanent toegankelijk moet zijn. Ook acht het college het noodzakelijk dat abonnees geïnformeerd worden over hoe zij hun aanbieder kunnen bereiken voor hulp of informatie over internetveiligheid.

8.4 Tijdstip informatieverstrekking

Het college hanteert de volgende criteria voor het moment van verstrekken van informatie:
– op het moment dat (toekomstige) abonnees de website van de aanbieder bezoeken,
– op het moment dat (toekomstige) abonnees een contract voor een dienst gaan afsluiten of verlengen,
– nadat er een substantiële wijziging in de bijzondere risico's optreedt, waarbij de individuele abonnee rechtstreeks benaderd dient te worden en de termijn waarbinnen deze informatie gestuurd wordt, recht doet aan de grootte van het risico.

8.5 Specifieke criteria voor informatie op websites

Sommige informatie kan zowel op papier als digitaal verstrekt worden. Indien de informatie te vinden is op de website van de aanbieder, dan hanteert het college de volgende criteria bij zijn toezicht:
1. op de website van de aanbieder is er een speciale pagina ingericht die algemene informatie geeft over veiligheid en beveiliging van internetdiensten;
2. op deze pagina worden de bijzondere en actuele veiligheidsrisico's benoemd en uitgelegd,[18] plus (een verwijzing naar) de eventuele middelen waarmee deze risico's kunnen worden tegengegaan alsmede een indicatie van de kosten;
3. op deze pagina staat een uitleg (of wordt verwezen naar een uitleg) van de gebruikte begrippen;
4. deze pagina is via maximaal 1 doorverwijzing ('één muisklik') te bereiken vanaf die pagina's waar de (toekomstige) abonnee als eerste terecht kan komen indien hij de dienst van deze aanbieder wil afnemen;[19]
5. de verwijzingen zijn gemakkelijk te vinden en benoemen duidelijk welke informatie met de verwijzing te vinden valt.

8.6 Overige middelen om informatie te verstrekken

Aanbieders kunnen naast het invullen van bovenstaande informatievoorziening ook nog andere middelen inzetten om hun abonnees te informeren. Zo zouden aanbieders hun informatievoorziening kunnen uitbreiden door op hun internetpagina of in hun andere communicatie aan abonnees de aandacht te vestigen op websites waarop veiligheidsrisico's en maatregelen worden behandeld, zoals bijvoorbeeld de website van Digibewust[20] of de waarschuwingsdienst van GOVCERT.NL[21].

---

[17] Ter toelichting een voorbeeld: een voorlichtingstekst als 'Om veilig te kunnen internetten zou u een firewall en een virusscanner moeten installeren op uw computer. U kunt hiervoor bijvoorbeeld het hiernaast afgebeelde pakket bij ons bestellen voor 50 Euro.' is naar het oordeel van het college niet afdoende. Immers, de abonnee wordt niet voorgelicht over de risico's die hij loopt als hij geen firewall en virusscanner installeert. Het begrip '(on)veilig internetten' is daarvoor niet expliciet genoeg.

[18] Hierbij heeft de aanbieder de vrijheid om inhoudelijke of verdiepende informatie op vervolgpagina's te vermelden zonder afbreuk te doen aan het overzicht voor de (toekomstige) abonnee.

[19] Dit kan bijvoorbeeld de *homepage* van de aanbieder pagina zijn, en/of de pagina van de webmaildienst en/of de pagina die het startpunt is voor de verkoop van internettoegangsdiensten. Het college maakt dit onderscheid, omdat een (toekomstige) abonnee op verschillende webpagina's van de aanbieder kan belanden. Soms kiest iemand ervoor om de homepage te zoeken, maar soms komt een abonnee via een banner op een andere pagina direct geleid naar een pagina waar een productaanbieding wordt gedaan (*landing page*). In dat geval zal deze *landingpage* dus een doorverwijzing naar de voorlichting moeten bevatten.

[20] Digibewust: www.digibewust.nl.

[21] Waarschuwingsdienst: www.waarschuwingsdienst.nl.

9 Handhaving

9.1 Algemeen

Op grond van de genoemde manieren van informatieverstrekking en de genoemde criteria die in het vorige hoofdstuk zijn genoemd, zal het college zowel ambtshalve toezicht houden (bijvoorbeeld met steekproeven) als toezicht houden op basis van klachten.

9.2 Klachten

Wat betreft het optreden op basis van klachten, geldt dat hoe meer klachten het college over een bepaalde schending van de informatieplicht binnenkrijgt, hoe groter de aanleiding voor het college is om ten aanzien van die betreffende schending handhavend op te treden. Eindgebruikers kunnen klachten indienen over een aanbieder die de informatieverplichting van artikel 11.3, tweede lid, Tw, overtreedt bij het loket van de overheid voor consumenten, de Consuwijzer.[22] Tevens zal het college klachten van specialisten en consumentenorganisaties in behandeling nemen.

9.3 Handhavingsmiddelen

Indien het college een overtreding van de Tw constateert, kan hij handhavend optreden. Het college beschikt hiertoe over de bestuurlijke handhavingsmiddelen last onder bestuursdwang, last onder dwangsom en de bestuurlijke boete. Daarnaast kan het college in voorkomende gevallen besluiten niet over te gaan tot het opleggen van een bestuurlijke sanctie, maar te volstaan met het geven van een waarschuwing.

9.4 Inzet van handhavingsmiddelen

Als het college een overtreding van de informatieplicht heeft geconstateerd, gaat hij in eerste instantie over tot het geven van een waarschuwing. Indien de overtreding vervolgens niet snel wordt beëindigd, zal het college overgaan tot het opleggen van een sanctie. Daarbij ligt een last onder dwangsom het meest voor de hand, omdat dit een herstelsanctie is. Dat betekent dat de sanctie is gericht op het beëindigen van een situatie die strijdig is met de wet. Het doel van de informatieplicht is om zorg te dragen dat abonnees worden geïnformeerd over bijzondere risico's en eventuele middelen waarmee deze risico's kunnen worden tegengegaan. Deze plicht wordt geschonden zolang de aanbieder deze informatie niet verstrekt. Door een last onder dwangsom op te leggen wordt de aanbieder gedwongen om alsnog aan de verplichting te voldoen en wordt het meest recht gedaan aan de doelstelling van artikel 11.3, Tw, de bevordering van veiligheid van abonnees.

Het opleggen van een boete is een strafsanctie, gericht op leedtoevoeging en is hier daarom veel minder op zijn plaats, tenzij er sprake is van een bijzonder ernstige overtreding of als de last onder dwangsom niet tot het gewenste resultaat leidt. De last onder bestuursdwang is volgens het college niet toepasbaar, omdat bij het inzetten van deze herstelsanctie het college bij een geconstateerde overtreding zelf de informatie moet gaan verzorgen. Dit betekent dat het college bijvoorbeeld zelf de website van de aanbieder zou gaan aanpassen.

10 Algemene slotbepalingen

10.1 Inherente afwijkingsbevoegdheid

Het college kan in bijzondere omstandigheden van dit beleid afwijken.

10.2 Aanpassing en herziening

Deze beleidsregels bevatten het OPTA-beleid inzake de handhaving van artikel 11.3, tweede lid, van de Telecommunicatiewet. Het college houdt zich uitdrukkelijk de mogelijkheid voor daarin wijzigingen aan te brengen. Toepassing van deze beleidsregels in de praktijk en voortschrijdend inzicht zullen zo nodig tot aanpassing of herziening ervan leiden.

[22] De Consuwijzer is te bereiken via de website www.consuwijzer.nl en via het telefoonnummer 088-0707070.

10.3 Inwerkingtreding

Deze beleidsregels treden in werking met ingang van de dag na publicatie ervan in de Nederlandse Staatscourant.

Het college van de Onafhankelijke Post en Telecommunicatie Autoriteit,
C.A. Fonteijn,
voorzitter.