Consultatie

Beleidsregels met betrekking tot de informatieplicht over veiligheid en beveiliging van aangeboden diensten en netwerken

---

1 Inleiding

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.[1] 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,[2] of over personen die ongemerkt PC's van anderen gebruiken voor criminele activiteiten.[3] 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.

De wetgever heeft in de Telecommunicatiewet (hierna: de Tw) meerdere artikelen opgenomen die als doel hebben de veiligheid van internetgebruik te vergroten. Artikel 11.3 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 van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college) heeft de taak toezicht te houden op de naleving van dit wetsartikel.

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,[4] een agentschap van de Europese Unie ten

---

[1] 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

[2] 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 vertrekken. De afzender van dit bericht deed zich voor als Zonnet. Zie http://www.websonic.nl/nieuws/062008/tele2_phishing_mail.php.

[3] Zie bijvoorbeeld het bericht van 2 augustus 2008 op http://www.techzine.nl/nieuws/17269/19-jarige-hacker-opgepakt-vanwege-verkoop-botnet.html.

[4] European Network and Information Security Agency.

behoeve van netwerk- en informatiebeveiliging, heeft onlangs een rapport[5] 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.

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[6] 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, deze staat centraal in deze consultatie. Wat betreft het tweede speerpunt is inmiddels duidelijk geworden dat er geen draagvlak bestaat bij ISP's voor het ontwikkelen van een keurmerk. Het college beraadt zich nog in overleg met het ministerie van Economische Zaken over alternatieve benaderingen van de beveiligingsplicht uit het eerste lid van artikel 11.3.[7] Wat betreft het laatste speerpunt (de aanpak van zombiecomputers) zijn recentelijk inventariserende gesprekken met ISP's gevoerd. Het college heeft positieve verwachtingen over de effecten van deze speerpunten op de veiligheid en beveiliging van internetdiensten.

Deze consultatie is als volgt opgebouwd. 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 gegeven. Hoofdstuk 4 en 5 gaan in op wat er aan informatie dient te worden gegeven of, in de woorden van artikel 11.3 Tw, welke bijzondere risico's in zijn ogen minimaal zouden moeten worden genoemd en welke middelen in aanmerking komen om deze risico's tegen te gaan. Vervolgens beschrijft het college achtereenvolgens op wie de informatieplicht berust en wie geïnformeerd dient te worden (hoofdstuk 6 en 7). Daarna geeft het college aan hoe en wanneer naar zijn mening een aanbieder de informatie dient te verstrekken (hoofdstuk 8) en beschrijft het college welke handhavingsmethoden hij wil gaan gebruiken (hoofdstuk 9). Tot slot volgt een uitleg van het verdere verloop van de consultatieprocedure (hoofdstuk 10).

[5] Security Economics and the Internal Market, R. Anderson et al., februari 2008.

[6] Tijdens de door ECP.nl georganiseerde bijeenkomst "Derde Kamer Discussie Zorgplicht" van 13 februari 2008.

[7] Zie hiervoor ook de brief aan ISP's, die op dezelfde dag als dit consultatiedocument op de website van OPTA is gepubliceerd.

2 Waarom beleidsregels voor de informatieplicht

Consumenten moeten zichzelf kunnen beschermen tegen de risico's van het gebruik van internet. Maar internet en internetdiensten kunnen zijn complex van aard. 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.[8]

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 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. Zulke aanbieders kunnen mogelijk vrezen voor inkomstenderving door goede voorlichting, omdat abonnees hun diensten gaan afnemen bij concurrerende aanbieders waar geen risico's vermeld worden. 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 de informatieplicht in te vullen. Alleen als iedereen zich inspant voor internetveiligheid zullen de risico's voor abonnees sterk afnemen. Een actieve rol van de toezichthouder is 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 beleidsregels. Het college wil zijn gedachten hierover graag voorleggen aan de markt en daarom consulteert hij in het onderhavige document zijn voorgenomen beleidsregels. Het college nodigt betrokken partijen en andere geïnteresseerden uit om op deze voorgenomen beleidsregels te reageren.

3 Juridisch kader

In de Privacy Richtlijn[9] (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

[8] 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.

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

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.

Artikel 4 van de Richtlijn luidt:

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.*

Artikel 11.3, Tw luidt:

1. *De in artikel 11.2 bedoelde aanbieders*[10] *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.*

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

In dit hoofdstuk wordt ingegaan op het begrip "bijzondere risico's" uit de informatieplicht van artikel 11.3, Tw. Het college verstaat onder deze risico's met name de risico's die een bijzondere band

[10] Bedoeld worden de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst.

hebben met de aard van het desbetreffende netwerk of de desbetreffende dienst.[11] Het college benoemt hieronder enkele concrete voorbeelden van risico's die minimaal geadresseerd dienen te worden door de aanbieder.

Risico	Technische term	Bijzondere band met de dienst
1. Het binnenkrijgen of (ongemerkt) versturen van grote hoeveelheden ongevraagde berichten).	spam	internettoegang, elektronische berichten, nieuwsgroepen, communitydiensten
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, nieuwsgroepen, communitydiensten
4. Het binnenkrijgen of (ongemerkt) versturen van software die bedoeld is om te spionneren op internetgedrag van abonnees.	*spyware*	internettoegang, elektronische berichten, nieuwsgroepen, communitydiensten
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, nieuwsgroepen, communitydiensten
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.	beveiliging draadloze modem	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, nieuwsgroepen, communitydiensten
8. Het bereikbaar zijn van of (ongevraagd) geconfronteerd worden met ongewenste	ongewenste websites	internettoegang

[11] Kamerstukken II, 1996/97, 25 533, nr. 3, p. 119.

websites, zoals websites die niet geschikt zijn voor kinderen.		

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.

Zoals in de derde kolom van de tabel is aangegeven, zullen niet al deze risico's altijd van toepassing zijn op iedere aanbieder. Bijvoorbeeld een aanbieder die louter een e-maildienst aanbiedt, heeft naar de mening van het college geen verplichting tot voorlichting over beveiliging van een draadloos netwerk.

1. *Deelt u de mening van het college dat bovenstaande veiligheids- en beveiligingsrisico's relevant zijn om abonnees over voor te lichten?*
2. *Kunt u andere veiligheidsrisico's benoemen die relevant zijn om abonnees over voor te lichten, maar die niet op bovenstaande lijst voorkomen?*

5 Middelen en indicatie van bijbehorende kosten

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 reëel 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. Het college acht de aanbieder als de partij die het best in staat is om de juiste middelen te benoemen en op de hoogte te zijn van de bijbehorende kosten om deze middelen in te zetten.

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 deze voorlichting dient de aanbieder de abonnee te informeren over hoe deze middelen de betreffende bijzondere risico's kunnen verkleinen.

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

3. *Wat is uw mening over het voornemen van het college om niet in beleidsregels vast te leggen hoe aanbieders abonnees informatie verstrekken over middelen om bijzondere risico's tegen te gaan?*

6 Aanbieders

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.[12] Daar de dienstaanbieders, in tegenstelling tot de netwerkaanbieders, een direct klantcontact hebben zal het college zich bij het toezicht op de naleving concentreren op de dienstaanbieders.

> *4. Wat is uw mening over het voornemen van het college om zich bij het toezicht op de naleving van de informatieplicht te concentreren op de dienstaanbieders?*

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 heeft het college het voornemen om zich bij het toezicht te 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.

> *5. Ziet u naast het internet nog andere diensten waarbij abonnees bijzondere veiligheid- en beveiligingsrisico's lopen waarover zij dienen voorgelicht te worden door hun aanbieder?*

7 Abonnees

De abonnees van een openbare elektronische-communicatiedienst kunnen zowel natuurlijke als rechtspersonen zijn.[13] 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 richt het college zich bij zijn toezicht op de mate waarin aanbieders informatie verstrekken aan abonnees uit de consumentenmarkt en het midden- en kleinbedrijf. Dat neemt niet weg dat het college, wanneer daar aanleiding toe is, handhavend zal optreden tegen een aanbieder die niet voldoende voorlichting geeft aan grootzakelijke abonnees.

[12] Kamerstukken II 1996/1997, 25 533, nr. 3, p.119.

[13] Artikel 1.1 onder p, van de Tw..

6. Wat is uw mening over de focus die het college legt op de informatievoorziening door aanbieders aan abonnees uit de consumentenmarkt en het midden- en kleinbedrijf?

8 De wijze van informatieverstrekking

In dit hoofdstuk licht het college zijn voornemen toe over hoe de informatie door de aanbieders zou moeten worden verstrekt aan de abonnees en hoe het college een overtreding van de informatieplicht zal handhaven.

Het college is van mening dat een aanbieder aan de gestelde informatieplichten voldoet indien de informatieverstrekking op een *duidelijke*, *ondubbelzinnige* en *voor leken begrijpelijke* manier plaatsvindt.

Verder is het college van mening dat de betreffende informatie *gemakkelijk*, *rechtstreeks* en *permanent toegankelijk* moet zijn en dat de informatie *actueel* en *relevant* gehouden wordt.

Ten derde is het college van mening dat de informatie minimaal verstrekt moet worden

- 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 abonnee rechtstreeks benaderd dient te worden en de termijn waarbinnen deze informatie gestuurd wordt, recht doet aan de grootte van het risico.

Tot slot is het college van mening dat abonnees geïnformeerd dienen te worden over hoe zij hun aanbieder kunnen bereiken voor hulp of informatie over internetveiligheid.

7. Wat is uw mening over bovengenoemde manieren van informatieverstrekking die het college maatgevend acht voor de bepaling of een aanbieder aan de informatieplicht voldoet?

De informatie kan zowel schriftelijk als digitaal verstrekt worden. Indien de informatie niet rechtstreeks aan de abonnee wordt geadresseerd,[14] maar te vinden is op de website van de aanbieder, dient deze naar de mening van het college aan de volgende voorwaarden te voldoen:

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, 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 de

[14] Bij rechtstreekse adressering kan gedacht worden aan informatie op de factuur, een nieuwsbrief, ed.

startpagina[15] van deze aanbieder.

5. De verwijzingen zijn duidelijk te vinden en benoemen duidelijk welke informatie met de verwijzing te vinden valt.

8. Wat is uw mening over bovenstaande criteria die het college wil gaan hanteren bij het bepalen of een aanbieder aan de informatieplicht voldoet?

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[16] of de waarschuwingsdienst van GOVCERT.NL[17].

9 Handhaving

Op grond van de genoemde manieren van informatieverstrekking en de genoemde criteria die in het vorige hoofdstuk zijn genoemd, zal het college op basis van klachten en steekproeven toezicht houden. Hoe meer klachten het college over een bepaalde schending van de informatieplicht binnenkrijgt, hoe groter de aanleiding is voor het college 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.[18] Tevens zal het college klachten van specialisten en consumentenorganisaties in behandeling nemen.

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.

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

[15] Bedoeld wordt de webpagina die bij de betreffende aanbieder voor de betreffende internetdienst het startpunt is voor (toekomstige) abonnees.

[16] Digibewust: www.digibewust.nl.

[17] Waarschuwingsdienst: www.waarschuwingsdienst.nl.

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

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.

9. Wat is uw reactie op hierboven beschreven methode van handhaving die het college voor ogen heeft?

10 Procedure

Het college nodigt u van harte uit om te reageren op de voorgenomen beleidsregels. Het college zal de reacties op deze consultatie meenemen bij het vaststellen van de definitieve beleidsregels en heeft het voornemen om deze definitieve beleidsregels in november te publiceren. Uw reactie zal een bijdrage kunnen leveren aan de kwaliteit van het toezicht van het college en daarmee aan de bescherming van persoonsgegevens en de persoonlijke levenssfeer van consumenten die van het internet gebruik maken.

Schriftelijke reacties kunt u binnen vier weken na publicatie van dit consultatiedocument sturen aan: OPTA, Postbus 90420, 2509 LK Den Haag. Het college verzoekt u om een afschrift van uw reactie te sturen aan zorgplicht@opta.nl. Mocht uw reactie vertrouwelijke gegevens bevatten dan dient u gemotiveerd aan te geven welke gegevens dat zijn.

Mocht u naar aanleiding van deze consultatie nog vragen hebben dan kunt u contact opnemen met dhr. H. Barnard of dhr. R. van den Broek via 070 -315 3500.