COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

College bescherming persoonsgegevens

Onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart tv door TP Vision Netherlands B.V.

z2012-00605

Openbare versie Rapport definitieve bevindingen

Juli 2013

INHOUDSOPGAVE

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar de wijze waarop TP Vision gegevens verzamelt en verwerkt over Nederlandse gebruikers van Philips smart tv's.

Een toenemend aantal Nederlandse huishoudens beschikt over een smart tv, een tv met internetdiensten. Het aanbod van *video on demand*-diensten groeit snel. Het toevoegen van een internetfunctionaliteit aan televisies heeft een wezenlijke verschuiving tot gevolg in het gegevensverkeer. Vroeger gaven televisies alleen tv-beelden door. Door de aansluiting op internet ontstaat tweerichtingsverkeer en de mogelijkheid voor (fabrikanten van) smart tv's om 'terug te kijken', het gedrag van kijkers te observeren en profielen van hen te maken.

Smart tv is een relatief nieuw fenomeen. Consumenten zullen zich daarom vaak niet bewust zijn van het feit dat wordt 'meegekeken' met hun televisiekijken, dat er analyses over hun kijkgedrag (kunnen) worden gemaakt en dat zij door bepaalde aanbiedingen of kijkaanbevelingen mogelijk beperkt worden in het maken van vrije keuzes.

De Wet bescherming persoonsgegevens (Wbp) stelt eisen aan het verwerken van persoonsgegevens. Mensen moeten zeggenschap hebben over hun eigen persoonsgegevens. Dat betekent bijvoorbeeld dat gebruikers van smart tv's geïnformeerd moeten zijn over het feit dat er persoonsgegevens van hen worden verzameld en wat daar verder mee wordt gedaan. Bij gebrek aan kennis over de gegevensverwerking kunnen zij hun rechten niet uitoefenen, zoals het intrekken van toestemming.

TP Vision verzamelt en bewaart persoonsgegevens
TP Vision verzamelt gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek (op hoofddomein) van de gebruikers van Philips smart tv's, onder meer door middel van cookies, en bewaart deze. Ook verzamelt en bewaart TP Vision per smart tv wanneer er tv wordt gekeken, welke uitzendingen en apps favoriet zijn, welke uitzendingen een gebruiker opneemt, welke video's een gebruiker huurt en welke 'uitzending gemist'-uitzendingen een betrokkene bekijkt. Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn. Dit soort gegevens zijn 'gevoelige' persoonsgegevens. De gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek etc. kunnen een indringend beeld kunnen geven van iemands communicatiegedrag en soms ook iets zeggen over de inhoud van de communicatie.

Overtredingen die nog niet zijn beëindigd

Informatieplicht
TP Vision is wettelijk verplicht gebruikers te informeren over de verwerking van hun persoonsgegevens. Zij moeten namelijk zicht (kunnen) hebben op het aantal en de soort verwerkingen die plaatsvinden met hun persoonsgegevens en de gevolgen daarvan, ook op de lange termijn.

TP Vision geeft gebruikers in Nederland onvolledige en onvoldoende duidelijke informatie over haar identiteit en over de gegevensverwerking via de Philips smart tv's. Voor een gebruiker van een Philips smart tv was (en is) het onvoldoende inzichtelijk wie TP Vision is, welke cookies en gegevens er worden geplaatst en uitgelezen door TP Vision en haar bewerkers, welke persoonsgegevens er worden verzameld en hoe lang deze persoonsgegevens worden bewaard. Ondanks herstelmaatregelen is TP Vision hierdoor (nog) in overtreding. De informatie in de gebruiksvoorwaarden, het Privacy Statement en de Cookie Policy was (en is) onvoldoende publiek toegankelijk en daarnaast inconsistent.

Daarnaast is onvoldoende duidelijk dat registratie van klantgegevens (bij Philips) optioneel is.

Cookies en toestemming
TP Vision plaatst gegevens op en leest informatie uit van Philips smart tv's, deels met behulp van cookies. Omdat het geen technisch noodzakelijke (zogeheten 'functionele') cookies betreft die uitgezonderd zijn van het toestemmingsvereiste uit de Telecommunicatiewet (Tw), moet TP Vision hiervoor geïnformeerde toestemming vragen en verkrijgen.

Hierbij vindt tegelijkertijd ook een verwerking van persoonsgegeven plaats. Voor die verwerking moet een wettelijke rechtvaardigingsgrond (grondslag) bestaan. In het geval van cookies waarmee het kijkgedrag wordt vastgelegd, is de enige rechtsgeldige grondslag ondubbelzinnige toestemming.

Wil er sprake zijn van rechtsgeldige toestemming, dan dient er sprake te zijn van een vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

TP Vision heeft op 18 april 2013 (voor nieuwe gebruikers), respectievelijk 2 juni 2013 (voor bestaande gebruikers) een toestemmingsvraag ingevoerd voor cookies die het kijkgedrag vastleggen, om persoonlijke kijkaanbevelingen te kunnen tonen. Door het ontbreken van volledige en duidelijke informatie voldoet de toestemming niet aan de criteria 'specifiek' en 'op informatie berustend'. Voor de advertentiecookies en de analytische cookies waarmee het appgebruik wordt vastgelegd, respectievelijk appgebruik en websitebezoek, vraagt TP Vision in het geheel geen toestemming. Hierdoor is het bedrijf in overtreding.

Bewerkerscontract
Op grond van de Wbp is een bedrijf verplicht een bewerkersovereenkomst te sluiten als een ander ten behoeve van het bedrijf persoonsgegevens verwerkt. TP Vision is in overtreding omdat zij geen bewerkersovereenkomst heeft gesloten met Google voor het verwerken van persoonsgegevens door Google Analytics.

Google heeft schriftelijk geweigerd een dergelijke overeenkomst aan te gaan. TP Vision heeft toegezegd de overtreding te zullen beëindigen door later dit jaar over te gaan op een eigen *analytics*-systeem.

Getroffen maatregelen en overtredingen die daardoor (gedeeltelijk) zijn beëindigd

Bewerkerscontracten
TP Vision maakt gebruik van de diensten van andere bedrijven voor de levering van de onlinediensten. Vier van deze bedrijven verwerken ten behoeve van TP Vision persoonsgegevens van de gebruikers van de smart tv's. Naar aanleiding van het onderzoek heeft TP Vision bewerkerscontracten gesloten met Gracenote, IBM en MPP Global (en indirect met Akamai). Door deze getroffen maatregel zijn de geconstateerde overtredingen op dit punt beëindigd.

Informatieplicht
Vanaf medio oktober 2012 heeft TP Vision een deel van de geconstateerde overtredingen met betrekking tot de informatieverstrekking verholpen. TP Vision heeft de gebruiksvoorwaarden uitgebreid met een Privacy Statement en een Cookie Policy. TP Vision heeft bovendien de gegevensverwerking gemeld bij het CBP. TP Vision heeft na ontvangst van het Rapport voorlopige bevindingen van het CBP informatie over de bewaartermijnen van de persoonsgegevens toegevoegd aan een nieuwe versie van het Privacy Statement en de Cookie Policy (per 1 mei 2013). Door deze getroffen maatregelen is de overtreding van de informatieplicht deels beëindigd.

1. INLEIDING

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek ingesteld naar de wijze waarop TP Vision Netherlands B.V. (hierna: TP Vision) gegevens verzamelt en verwerkt over gebruikers in Nederland van Philips smart tv's.

Aanleiding onderzoek

Een toenemend aantal Nederlandse huishoudens beschikt over een smart tv, een tv met internetdiensten. Onderzoeksbureau iMMovator schrijft: "*Het gebruik van video on demand diensten groeit snel en wordt snel meer divers. In 2011 was 34 procent (610.000 exemplaren) van alle verkochte televisies een web-tv. De verwachting is dat dit in 2012 oploopt tot 60 procent. Eén op de drie huishoudens kan dan via z'n televisie gebruik maken van nieuwe diensten via het portal van de televisiefabrikant, via speciale "apps" of via directe toegang tot het internet. Eind 2013 zal de helft van de huishoudens via hun televisie IP-connected zijn* (…)."[1]

Het aanbod van *video on demand*-diensten groeit snel. Het toevoegen van een internetfunctionaliteit aan televisies heeft een wezenlijke verschuiving tot gevolg in het gegevensverkeer. Vroeger gaven televisies alleen tv-beelden door. Door de aansluiting op internet ontstaat tweerichtingsverkeer en de mogelijkheid voor (fabrikanten van) smart tv's om 'terug te kijken', het gedrag van kijkers te observeren en profielen van hen te maken.

Dat kijkgedrag geanalyseerd wordt, blijkt onder meer uit uitspraken in de media over de Philips smart tv. Een verantwoordelijk manager bij Koninklijke Philips Electronics N.V. (hierna: Philips) zei in februari 2012 dat het bedrijf registreerde hoe vaak Nederlandse gebruikers hun smart tv gebruiken. "*Nu al zet meer dan 60 procent van de actieve Philips Smart TV-gebruikers de Smart TV meer dan vijftig keer per maand aan.*"[2] Op 1 september 2012 vulde het hoofd smart tv van TP Vision aan dat 80% van de Philips smart tv's in Nederland al was aangesloten op internet. "*Wij zien een enorme toename van het gebruik. In januari hebben wij nog gecommuniceerd dat zestig procent van de gebruikers minstens een keer per dag een app gebruikt, nu is dat 75 procent.*"[3] Tevens gaf hij aan een top 10 bij te houden van meest gebruikte apps. In reactie op de vraag in hoeverre deze activiteiten inkomsten genereren, antwoordde deze manager: "*Smart tv*

[1] iMMovator, kwartaalrapportage digitale televisie maart 2012, 'Connected TV-diensten worden de drijver voor de digitale televisiemarkt', 12 maart 2012, URL: http://www.immovator.nl/connected-tv-diensten-worden-de-drijver-voor-de-digitale-televisiemarkt. Volgens het Centraal Bureau voor de Statistiek had eind 2012 1 op de 5 huishoudens in Nederland een smart tv. Bron: Persbericht CBS, 25 januari 2013, URL: http://www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2013/2013-3772-wm.htm.

[2] Persbericht TP Vision, 'Philips TV verbreedt zijn Smart TV reeks en personaliseert de gebruikersbeleving verder', 20 februari 2012, URL: http://www.tpvision.nl/pr/press-release/philips-tv-verbreedt-zijn-smart-tv-reeks-en-personaliseert-de-gebruikersbeleving.

[3] Emerce, Philips: 'Smart TV is serieuze business', 1 september 2012, URL: http://www.emerce.nl/nieuws/philips-smart-tv-serieuze-business.

is business, laat dat duidelijk zijn. Adverteerders stappen er nu serious in, er worden grote budgetten voor vrijgemaakt."

Organisatiebeschrijving

TP Vision houdt zich bezig met het design, de productie, de distributie, marketing en verkoop van de Philips smart tv's. Het bedrijf is gevestigd te Amsterdam en houdt kantoor te Amsterdam en Eindhoven. Philips bezit 30% van de aandelen, TPV Technology Limited uit Hong Kong bezit 70% van de aandelen in de joint venture.

Onderzoeksvragen

Het onderzoek van het CBP heeft zich geconcentreerd op de volgende vragen.

- Verwerkt TP Vision gegevens met betrekking tot het kijk- en internetgedrag van gebruikers in Nederland van een Philips smart tv? Zo ja, zijn dit persoonsgegevens als bedoeld in artikel 1, aanhef en onder a, van de Wbp?
- Heeft TP Vision een grondslag voor de verwerking(en) van deze persoons-gegevens, als bedoeld in artikel 8 van de Wbp?
- Informeert TP Vision gebruikers van de Philips smart tv over de gegevensverwerking(en), als bedoeld in de artikelen 33 en/of 34 van de Wbp?
- Zijn de bedrijven waarmee TP Vision samenwerkt, bewerkers als bedoeld in artikel 1, aanhef en onder e, van de Wbp? Heeft TP Vision (een) bewerkersovereenkomst(en) gesloten als bedoeld in artikel 14 van de Wbp?
- Indien TP Vision gegevens plaatst en/of uitleest op Philips smart tv's, krijgt TP Vision hiervoor dan toestemming van de gebruikers, als bedoeld in artikel 11.7a van de Tw?

Verloop onderzoek

Het CBP heeft, na telefonisch overleg met het hoofd smart tv van TP Vision, per e-mail van 13 september 2012 aangekondigd om onderzoek ter plaatse in te stellen bij het bedrijf. Bij brief van 20 september 2012 heeft het CBP het onderzoek nader toegelicht, vergezeld van een lijst van vragen die tijdens het onderzoek aan de orde zouden komen.

Het onderzoek ter plaatse heeft plaatsgevonden op 9 oktober 2012, in het kantoor van TP Vision in Eindhoven. TP Vision heeft een groot deel van de vragen schriftelijk beantwoord en deze antwoorden op 9 oktober bij aanvang van het onderzoek ter plaatse aan het CBP overhandigd. Tijdens het onderzoek ter plaatse heeft TP Vision deze antwoorden nader toegelicht. Bij brief van 16 oktober 2012 heeft het CBP een aantal relevante mondelinge verklaringen over de gegevensverwerking schriftelijk bevestigd en verzocht de ontbrekende gevraagde stukken uiterlijk 22 oktober 2012 aan het CBP te verstrekken. TP Vision heeft het CBP bij e-mail van 15 oktober een Privacy Statement en Cookie Policy toegestuurd en aangegeven een melding te doen van de gegevensverwerking bij het CBP. Per fax en e-mail van 18 oktober 2012 heeft TP Vision gereageerd op de weergave van de mondelinge verklaringen en één van de toegezegde stukken verstrekt. De overige gevraagde stukken zijn op 23 oktober 2012 aan het CBP verstrekt. Per e-mail van 29 oktober 2012 heeft TP Vision twee laatste openstaande vragen van het CBP beantwoord.

Op 12 december 2012 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen, met het verzoek deze uiterlijk 14 januari 2013 te verstrekken. Op 2 januari 2013 heeft het CBP de vragen telefonisch toegelicht. TP Vision heeft een groot deel van de gevraagde inlichtingen per e-mail van 14 januari 2013 en per koerier op 16 januari 2013 verstrekt. Aanvullend heeft TP Vision stukken aan het CBP verstrekt per e-mail, op 5, 6, 12 en 18 februari 2013. Op 25 februari 2013 heeft het CBP controlerend onderzoek gedaan op een nieuwe Philips smart tv (aangeschaft op 2 februari 2013).

Het CBP heeft op 7 maart 2013 het Rapport voorlopige bevindingen vastgesteld. Het CBP heeft TP Vision bij brief van 7 maart 2013 in de gelegenheid gesteld om haar zienswijze op het Rapport voorlopige bevindingen naar voren te brengen.

TP Vision heeft bij brief van 5 april 2013 zijn zienswijze gegeven en aangekondigd uiterlijk 8 mei 2013 aanvullende inlichtingen te geven over maatregelen om geconstateerde overtredingen te beëindigen.

Op 8 april 2013 heeft het CBP telefonisch contact opgenomen met TP Vision.

Bij brief van 10 april 2013 heeft het CBP een toelichting verstrekt op de beoordeling van een bewerkerscontract in het Rapport voorlopige bevindingen en een aanvullende vraag gesteld aan TP Vision.

Bij brief van 8 mei 2013 heeft TP Vision de toegezegde inlichtingen verstrekt en gereageerd op de aanvullende vraag van het CBP.

Op 15 mei 2013 heeft het CBP telefonisch contact opgenomen met TP Vision en aangegeven uiterlijk 3 juni 2013 aanvullend onderzoek te doen op een Philips smart tv teneinde de definitieve bevindingen te kunnen opmaken.

Op 3 juni 2013 heeft het CBP een tweede controle-onderzoek gedaan op de Philips smart tv van een bestaande gebruiker (aangeschaft op 2 februari 2013).

Op 5 juni 2013 heeft het CBP telefonisch inlichtingen ingewonnen bij TP Vision.

Op 26 juni 2012 heeft het CBP de wetsuitleg/-toepassing in het Rapport definitieve bevindingen waar het gaat om artikel 11.7a van de Tw afgestemd met de Autoriteit Consument en Markt (ACM).

Op 2 juli 2013 heeft het CBP het Rapport definitieve bevindingen vastgesteld.

Zienswijze TP Vision op Rapport voorlopige bevindingen CBP

In haar zienswijze van 5 april 2013 op het Rapport voorlopige bevindingen van 7 maart 2013, aangevuld bij brief van 8 mei 2013, brengt TP Vision, samengevat weergegeven, naar voren dat TP Vision gegevens verzamelt over de televisies en het algemene gebruik daarvan, maar dat dit niet automatisch persoonsgegevens zijn, omdat TP Vision niet weet wie er voor de televisie zit.[4]

[4] Zienswijze TP Vision van 5 april 2013, p. 2.

IP-adressen zijn voor TP Vision evenmin per definitie persoonsgegevens, omdat ze zonder aanvullende identificerende gegevens niet herleidbaar zijn naar een identificeerbare natuurlijke persoon.[5] Volgens TP Vision zijn IP-adressen in feite 'gecodeerde gegevens' als bedoeld in de memorie van toelichting bij de Wbp, en beschikt TP Vision niet "*over de middelen om zonder veel moeite de tenaamstelling en adresgegevens behorend bij een IP nummer te achterhalen.*"[6]

De gebruikte Google Analytics-cookies zijn voor TP Vision geen *tracking* cookies, omdat de code uitsluitend op de webpagina van de '*APP gallery*' in het Service Portal is geïmplementeerd, en er dus slechts sprake is van één dienst van de informatiemaatschappij. "*Doordat TP Vision IP-masking heeft ingesteld wordt het laatste byte (of 'octet') van het IP adres dat Google ontvangt automatisch verwijderd voordat Google dit opslaat. Omdat TP Vision tevens de optie van 'gegevens delen' heeft uitstaan, worden de opgeslagen gegevens van televisies door Google uitsluitend gebruikt ten behoeve van de levering van Google Analytics rapporten aan TP Vision.*"[7] TP Vision geeft aan voornemens te zijn Google Analytics in te ruilen voor een eigen systeem en verwacht "*dat dit nieuwe systeem later dit jaar operationeel zal zijn*."[8]

TP Vision geeft aan geen uitvoerige theoretische discussie te willen voeren over de definitie van persoonsgegevens in het rapport. "*Zonder erkenning van enig standpunt uit uw Rapport, zal TP Vision de door u in de tabel van paragraaf 3.2 van uw Rapport genoemde gegevens integraal meenemen bij de verdere aanpassing van de processen die ertoe zullen leiden dat de door u geconstateerde tekortkomingen worden verholpen.*"[9] De aanpassingen zullen geen betrekking hebben op Google Analytics.

TP Vision noemt drie concrete actiepunten die volgens haar nodig zijn om de geconstateerde overtredingen te beëindigen en zegt toe het CBP op 8 mei 2013 op de hoogte te stellen van de voortgang met betrekking tot deze actiepunten.

De drie actiepunten zijn:

- "vaststellen van de laatste details (inclusief bewaartermijnen) voor, en afsluiten van, bewerkersovereenkomsten met Gracenote, IBM en Philips;
- aanpassen van Smart TV Privacy Statement en Cookie Policy met bewaartermijnen;
- activeren van goedkeuringsscherm voor de recommender dienst."[10]

TP Vision wijst in haar zienswijze op een aantal feitelijke onjuistheden en verwijzingen in het feitelijk kader van het rapport.[11]

[5] Idem, p. 3.
[6] Idem, p. 4.
[7] Idem, p. 5.
[8] Idem, p. 11.
[9] Idem, p. 10.
[10] Idem, p. 17.
[11] Idem, 7-8.

TP Vision geeft in haar zienswijze aan druk bezig te zijn met het opstellen en (laten) ondertekenen van (uitgebreidere) bewerkersovereenkomsten met Philips, GraceNote en IBM.

Begin maart 2013 heeft TP Vision een herhaald verzoek tot ondertekening van die bewerkersovereenkomst aan Philips gestuurd.[12] Naderhand heeft TP Vision aangegeven dat Philips geen gegevens deelt met TP Vision, niet voor marketing en niet voor interne onderzoeksdoeleinden, en dat daarom geen sprake is van een bewerkersrelatie en evenmin van een gezamenlijke verantwoordelijkheid. "*Mochten de plannen met betrekking tot dergelijk gebruik wijzigen, dan zullen TP Vision en Philips eerst een bewerkersovereenkomst tekenen.*"[13]

Begin mei 2013 heeft TP Vision de definitieve en ondertekende versies van de overeenkomsten met GraceNote en IBM toegestuurd aan het CBP.[14] Daarbij heeft TP Vision, in relatie tot Akamai, de passage over subbewerkers in het contract met IBM uitgebreid. "*Mede gelet op uw Rapport, heeft TP Vision in haar laatste herinnering aan IBM de clause betreffende het sub-bewerkersschap in de concept-overeenkomst nog aangescherpt, zodat de normen en voorwaarden (…) ook dwingend gaan gelden op de relatie tussen bewerker en sub-bewerker.*"[15] TP Vision geeft aan dat met IBM "*op korte termijn een additionele overeenkomst in lijn met de 'Standard Contractual Clauses' worden ondertekend, omdat gebleken is dat data eventueel ook naar servers buiten de EU worden verzonden.*"[16] Telefonisch heeft TP Vision toegelicht dat zij verwacht deze clauses eind juni 2013 aan het CBP te kunnen toesturen.[17]

Ten aanzien van Google Analytics merkt TP Vision op dat Google niet bereid is tot het aangaan van een bewerkersovereenkomst en dat TP Vision voornemens is later dit jaar een eigen systeem voor analytics in gebruik te nemen.[18] Aanvullend heeft TP Vision een afschrift verstrekt van deze schriftelijke weigering door Google.[19]

Ten aanzien van de bewerkersovereenkomst met MPP Global heeft TP Vision nadere duiding gevraagd van het CBP waarom de overeenkomst niet zou voldoen aan de vereisten van artikel 14 van de Wbp.[20] Begin mei 2013 heeft TP Vision aanvullende informatie (achterliggende documenten) verstrekt over deze bewerkers-overeenkomst.[21]

TP Vision geeft aan de beschikbaarheid van de informatie over haar identiteit en de aard van de gegevensverwerking te hebben verbeterd door vernieuwing van haar eigen website en bezig te zijn met verbetering van de vindbaarheid via de websites

[12] Idem, p. 9.
[13] Brief TP Vision van 8 mei 2013, p. 3.
[14] Idem, bijlages 1 en 2.
[15] Zienswijze TP Vision van 5 april 2013, p. 12.
[16] Brief TP Vision van 8 mei 2013, p. 1
[17] Telefonische inlichting TP Vision 5 juni 2013.
[18] Zienswijze TP Vision van 5 april 2013, p. 11
[19] Idem, bijlage 3.
[20] Idem, p. 13.
[21] Brief TP Vision van 8 mei 2013, bijlages 8 en 9.

van Philips.[22] Begin mei 2013 heeft TP Vision een voorbeeld gestuurd van een verwijzing op een specifieke webpagina van Philips.[23] TP Vision schrijft: "*Als volgende stap zal de beschikbaarheid van de vraag* [naar privacy op Philips smart tv's, toevoeging CBP] *worden uitgebreid, en uiteindelijk zullen het Privacy Statement en de Cookie Policy als aparte documenten bovenaan de 'ondersteunings-tab' worden opgenomen (waar nu al de gebruikershandleiding etc. zijn opgenomen).*"[24]

Ten aanzien van het toestemmingsvereiste voor het plaatsen en uitlezen van bepaalde soorten cookies, schrijft TP Vision dat vanaf 22 april 2013 aan nieuwe gebruikers ondubbelzinnige toestemming wordt gevraagd voor het gebruik van de cookies en dat TP Vision "*het systeem verder* [zal, toevoeging door het CBP] *aanpassen zodat ook de bestaande gebruikers een scherm te zien gaan krijgen waarin expliciet om toestemming wordt gevraagd*."[25] Naderhand heeft TP Vision verklaard dat de wijzigingen eerder in werking zijn getreden en dat nieuwe gebruikers (en gebruikers die hun toestel resetten) sinds 18 april 2013 het opt-inscherm te zien krijgen.

Het aanbieden van een pop-up-scherm voor bestaande gebruikers bleek technisch complexer, maar zou "*binnen enkele weken operationeel zijn*."[26]

Ten aanzien van de bewaartermijn geeft TP Vision aan in samenspraak met de bewerkers de bewaartermijnen in kaart te brengen en 'binnen een maand' te vermelden in aangepaste versies van het privacystatement en de cookiepolicy.[27]

Over het registratiescherm voor 'Club Philips' verklaart TP Vision dat de opmerking over software-updates is verwijderd uit het scherm.[28] Daarnaast 'versnelt' TP Vision 'de meer algemene aanpassing van de Smart TV Terms of Use', waarbij tevens de wijze waarop deze op de televisie worden getoond aan bod komt, "*zodat gebruiker beter wordt ingelicht en zijn of haar geduld minder op de proef wordt gesteld*."[29]

Bevoegdheid CBP

Op de verwerking van persoonsgegevens is de Wet bescherming persoonsgegevens van toepassing.

Op grond van artikel 60, eerste lid, van de Wbp kan het CBP ambtshalve of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.

[22] Zienswijze TP Vision van 5 april 2013, p. 13-14.
[23] Brief TP Vision van 8 mei 2013, bijlage 6.
[24] Idem, p. 2
[25] Zienswijze TP Vision van 5 april 2013, p. 14
[26] Brief TP Vision van 8 mei 2013, p. 2.
[27] Zienswijze TP Vision van 5 april 2013, p. 15.
[28] Idem, p. 16
[29] Idem, p. 17.

De toezichthoudende taak van het CBP is niet beperkt tot het terrein van de Wbp, maar strekt zich ook uit tot andere wetten, algemene maatregelen van bestuur en andere regelingen op grond waarvan persoonsgegevens worden verwerkt.

Volgens artikel 51, eerste lid, van de Wbp, jo. artikel 61, eerste lid, van de Wbp, ziet het CBP toe *op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde.*

Het CBP ziet ook toe op de naleving van de bepalingen uit hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegeven in de sector elektronische communicatie.[30]

In de wetsgeschiedenis bij de Wbp is hierover het volgende opgemerkt:

> *"Op grond van artikel 51 van het voorliggende wetsvoorstel wordt het Cbp belast met het toezicht op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens de wet bepaalde. Dit betekent dat het Cbp een algemene toezichtsbevoegdheid heeft die zich niet alleen uitstrekt tot de naleving van het bij of krachtens het voorstel voor een Wet bescherming persoonsgegevens bepaalde, maar ook tot hetgeen bij of krachtens hoofdstuk 11 van het voorstel voor een Telecommunicatiewet is bepaald, voor zover het de verwerking van persoonsgegevens betreft. (…) De OPTA is ook belast met toezicht op de naleving en de bestuursrechtelijke handhaving van hoofdstuk 11* [van de Tw, toevoeging door het CBP]. *Die bevoegdheden zullen met name betekenis hebben voor zover het niet de verwerking van persoonsgegevens betreft."*[31]

[30] Kamerstukken II 2002/03, 28 851, nr. 7, p. 53-54.

[31] Kamerstukken II 1998/99, 25 892, nr. 6, p. 43. Zie Kamerstukken II 2002/03, 28 851, nr. 3, p. 61: "Het CBP is op grond van de Wbp belast met het toezicht op de naleving van de Wbp in het algemeen, en waar het de verwerking van persoonsgegevens door aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten op grond van hoofdstuk 11 Telecommunicatiewet betreft, ook op die bepalingen. Daarnaast is het college [van OPTA, toevoeging door het CBP] op basis van hoofdstuk 15 Telecommunicatiewet belast met het toezicht op hoofdstuk 11 Telecommunicatiewet als geheel. De nadruk in het toezicht van het college ligt echter op andere aspecten van hoofdstuk 11 Telecommunicatiewet dan die waarop het CBP toeziet." Zie ook Kamerstukken I 2003/04, 28 851, nr. C, p. 34; Kamerstukken II 2002/03, 28 851, nr. 7, p. 43 en Kamerstukken II 1997/98, 25 533, nr. 5, p. 117.

2. BEVINDINGEN

2.1 Uitwerking van het wettelijk kader

2.1.1 Verantwoordelijke

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.*

Uit de definitie volgt dat een verantwoordelijke "te zamen met anderen" verantwoordelijk kan zijn voor de gegevensverwerking. Daarbij kunnen drie vormen van gedeelde verantwoordelijkheid worden onderscheiden. In de wetsgeschiedenis bij de Wbp is hierover het volgende opgemerkt:

"*1. Aan de verwerkingen nemen verschillende organisaties deel, er is echter één gemeenschappelijke verantwoordelijke. Deze is aansprakelijk voor de verwerkingen als geheel. Daarnaast zijn de deelnemende organisaties aansprakelijk voor de aangeleverde gegevens. De verantwoordelijke is voor de inhoud daarvan slechts verantwoordelijk naar de mate waarop hij daarover juridische zeggenschap heeft. (...)*
2. Verschillende verwerkingen zijn min of meer geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van afzonderlijke verantwoordelijkheid per (deel-)verwerking. De betrokkene kan slechts één van de afzonderlijke verantwoordelijken aanspreken. (…)
3.Verschillende verwerkingen zijn geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van gezamenlijke verantwoordelijkheid. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerkingen."[32]

2.1.2 Persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan: *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*.

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en omvat onder meer het verzamelen, vastleggen, bewaren, gebruiken, samenbrengen en met elkaar in verband brengen van persoonsgegevens.[33]

Artikel 1, aanhef en onder a, van de Wbp vormt een implementatie van artikel 2, aanhef en onder a, van de Privacyrichtlijn:

[32] Kamerstukken II 1998/99, 25 892, nr. 3, p. 58.
[33] Artikel 1, aanhef en onder b, van de Wbp verstaat - voluit - onder 'verwerking van persoonsgegevens': "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens".

> *"In de zin van deze richtlijn wordt verstaan onder (…) "persoonsgegevens", iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene" te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.*"

Overweging 26 van de Privacyrichtlijn luidt in dit verband:

> *"Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is; dat de gedragscodes in de zin van artikel 27 een nuttig instrument kunnen zijn om een indicatie te geven omtrent de middelen waarmee de gegevens anoniem kunnen worden gemaakt en kunnen worden bewaard in een vorm die identificatie van de betrokkene niet langer mogelijk maakt."*

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd.[34]

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking[35] hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of – gezien de context[36] waarin ze worden verwerkt – medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.[37] In dat laatste geval is het gebruik dat van de gegevens kan worden gemaakt medebepalend voor de beantwoording van de vraag of sprake is van

[34] Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.
[35] Zie Artikel 29-werkgroep WP 136. Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, p. 10-11 en 27, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf: "Er is sprake van informatie "betreffende" een persoon wanneer het gaat om informatie "over" die persoon", met andere woorden, de inhoud. Idem, p. 11
[36] Vgl. idem: Er is sprake van informatie 'betreffende' een persoon "wanneer, rekening houdende met alle omstandigheden van het precieze geval, gegevens worden gebruikt of waarschijnlijk zullen worden gebruikt met het doel een persoon te beoordelen, op een bepaalde wijze te behandelen of de status of het gedrag van die persoon te beïnvloeden", met andere woorden, het doel.
[37] Kamerstukken II 1997/98, 25 892, nr. 3, p. 46. Vgl. idem: Er is sprake van informatie 'betreffende' een persoon "indien het gebruik ervan, rekening houdende met alle omstandigheden van het geval, naar verwachting gevolgen zal hebben voor iemands rechten of belangen", met andere woorden, het resultaat.

een persoonsgegeven.[38] Ook gegevens die niet direct betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen over een bepaalde persoon informatie verschaffen en zijn in dat geval persoonsgegevens.[39]

Een persoon is identificeerbaar indien zijn identiteit – direct of via nadere stappen, door gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor zijn persoon[40] – redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.[41] Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren.[42] Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke. [43] In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.[44]

De Artikel 29-werkgroep, het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders, heeft over het begrip persoonsgegeven in dat verband

[38] Idem, p. 47. "Anders dan de Registratiekamer in haar advies stelt is niet vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt. Indien het daarentegen mogelijk is de gegevens te gebruiken bij voorbeeld om fraude op te sporen, dan is er sprake van persoonsgegevens. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken, ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt" (onderstreping toegevoegd door het CBP).
[39] Idem, p 46-47.
[40] Idem, p. 48. Bijvoorbeeld "gevallen (…) waarbij gegevens niet direkt op naam zijn terug te vinden, doch de betrokken persoon met aanwending van beschikbare middelen alsnog kan worden achterhaald, bijvoorbeeld aan de hand van een nummer. Te denken valt aan een situatie waarbij een lijst van nummers met bijbehorende namen beschikbaar is, hetzij via openbare bron, (bijvoorbeeld het telefoonboek), hetzij via een bron die slechts raadpleegbaar is voor een bepaalde categorie van personen (bijvoorbeeld het kentekenregister door de politie of het nummer van een rekening door bankemployés). De met die nummers verbonden gegevens zijn - hoewel niet op naam - persoonsgegevens wegens de beschikbare mogelijkheid om met behulp van de nummers de identiteit van de betrokken personen te achterhalen", Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.
[41] Idem, nr. 3, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip 'onevenredige inspanning' opgemerkt: "Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen." Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.
[42] Idem, nr. 3, p. 48. Daarbij moet rekening worden gehouden met alle relevante factoren, zoals de kosten van identificatie, het beoogde doel van de verwerking, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico op organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen. Artikel 29-werkgroep 136. Advies 4/2007 over het begrip persoonsgegeven, van 20 juni 2007, p. 16.
[43] Kamerstukken II 1998/99, 25 892, nr. 3, p. 48-49.
[44] Idem, p. 49. Registratiekamer 27 maart 1995, 95.V.029.

opgemerkt dat het niet in alle gevallen noodzakelijk is om de naam van een betrokkene te kennen om vast te stellen dat het om persoonsgegevens gaat.[45]
De Artikel 29-werkgroep schrijft: *"(…) dat hoewel identificatie door middel van de naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan de geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook van de gebruiker ervan. De persoonlijkheid van de betrokkene kan op deze wijze worden achterhaald, zodat bepaalde besluiten aan hem of haar kunnen worden toegeschreven. Zonder zelfs maar naar de naam en het adres van de persoon te vragen, kan de betrokkene worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde beslissingen aan hem of haar worden toegeschreven, omdat het voor het contactpunt voor de persoon (de computer) niet langer nodig is zijn of haar identiteit in enge zin bekend te maken. Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van "persoonsgegeven" weerspiegelt ook dit feit."*[46]

De Artikel 29-werkgroep geeft daarbij aan dat ook sprake is van persoonsgegevens als het doel van de verwerking juist gericht is op identificatie van personen.

"In dergelijke gevallen waarin het doel van de verwerking impliceert dat personen worden geïdentificeerd, kan worden verondersteld dat de voor de verwerking verantwoordelijke over "redelijkerwijs in te zetten middelen" beschikt om de betrokkene te identificeren. Aan te voeren dat personen niet identificeerbaar zijn als het doel van de verwerking nu juist die identificatie is, komt neer op een contradictio in terminis. De informatie moet dan ook worden beschouwd als informatie betreffende identificeerbare personen, wat betekent dat voor de verwerking de regels inzake gegevensbescherming gelden."[47]

2.1.3 Gegevensverwerking
Het begrip 'verwerking van persoonsgegevens' omvat het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen tot aan het moment van vernietiging.[48] Ook het genereren van persoonsgegevens is een verwerking.[49] Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze

[45] Zie ook HvJ EG 6 november 2003, zaak C-101/01 (Lindqvist), r.o. 27: "(…) het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, [is, toevoeging door het CBP] als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens in de zin van artikel 3, lid 1, van richtlijn 95/46 (…) aan te merken."
[46] Artikel 29-werkgroep 136. Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, p. 16-17.
[47] Idem.
[48] Zie Kamerstukken II 1997/98, 25 892, nr. 3, p. 51-52.
[49] Idem, p. 51

gegevens.[50] Ook volledig geautomatiseerde vormen van gegevensverwerking vormen een verwerking, zo lang (enige) invloed daarop uit kan worden geoefend.[51]

2.1.4 Bewerkersovereenkomst

De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder dat hij diens ondergeschikte is. De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid.[52] Het bewerkersbegrip is van toepassing op verschillende vormen van dienstverlening. Uitgangspunt is daarbij dat de dienstverlening betrekking heeft op het verwerken van persoonsgegevens.[53]

Op grond van artikel 14 van de Wbp, voor zover voor dit onderzoek van belang, dient een verantwoordelijke die persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, zorg te dragen dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.

De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

In de artikelen 12 en 14 van de Wbp wordt de rechtsbetrekking tussen verantwoordelijke en bewerker nader ingevuld.

Artikel 14 Wbp gaat over de relatie verantwoordelijke - bewerker en de verplichting om een overeenkomst tussen de verantwoordelijke en de bewerker op te stellen. De ratio van deze bepaling is dat de wetgever heeft willen voorkomen dat bij eventuele

[50] Van verzameling is al sprake indien de gegevens worden verkregen en vervolgens onmiddellijk worden vernietigd. Kamerstukken II 1997/98, 25 892, nr. 3, p. 68.

[51] Kamerstukken II 1997/98, 25 892, nr. 3, p. 68: "Zodra er enige feitelijke macht over persoonsgegevens is, is het wetsvoorstel van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking kunnen onder de wettelijke regeling vallen. Cruciaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige) invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend. Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing" (onderstreping toegevoegd door het CBP).

[52] Idem, p. 61.

[53] Idem, p. 62.

tekortkomingen in de gegevensverwerking verantwoordelijke en bewerker zich wat betreft hun verantwoordelijkheden achter elkaar zouden kunnen verschuilen.[54]

Bepalend voor de afbakening van het begrip bewerker is de relatie met de verantwoordelijke voor de gegevensverwerking en de mate van zeggenschap waarmee de verwerking van persoonsgegevens gepaard gaat.[55]

De bewerker beperkt zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens.[56] In het advies van de Artikel 29-werkgroep over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker' wordt dit uitgangspunt enigszins genuanceerd. Het vaststellen van de 'middelen' voor de verwerking kan door de voor de verwerking verantwoordelijke worden gedelegeerd wanneer het gaat om technische of organisatorische maatregelen. Kernvragen met betrekking tot de rechtmatigheid van de verwerking vallen onder de bevoegdheid van de voor de verwerking verantwoordelijke.[57] De bewerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers en de duur van de opslag van de gegevens. Zou hij immers deze zeggenschap wel verwerven, dan dient hij als verantwoordelijke te worden aangemerkt.[58]

Artikel 14 Wbp regelt formele en materiële vereisten waaraan een bewerkersovereenkomst dient te voldoen.

De formele vereisten zijn als volgt.

Er dient sprake te zijn van een overeenkomst of een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke. Met andere woorden, de verantwoordelijke en de bewerker dienen partij bij de overeenkomst te zijn. Bovendien moet het gaan om een juridisch bindend voorschrift in schriftelijke of in een andere, gelijkwaardige vorm.[59] Het kan niet gaan om mondelinge afspraken.[60]

Ten aanzien van de materiële vereisten geldt het volgende.

De overeenkomst moet naar zijn aard betrekking hebben op de gegevensverwerking. Het contract mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is.[61]

---

[54] Zie Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.
[55] Idem, p. 61.
[56] Idem, p. 61-62.
[57] Artikel 29-werkgroep WP 169, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf
[58] Zie Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61 en 62.
[59] Idem, p. 99.
[60] Idem, p. 100.
[61] Idem, p. 99.

De verplichtingen moeten over en weer duidelijk zijn neergelegd in de bewerkersovereenkomst.[62] Niet alleen dient de verantwoordelijke civielrechtelijk de bewerker voldoende te hebben duidelijk gemaakt hoe met de persoonsgegevens wordt omgegaan, tevens dient hij toe te zien op de feitelijke naleving van de aldus gecreëerde verplichtingen.[63] Van belang is dat de verantwoordelijke zelf bepaalt welke soort gegevens hij verwerkt, hoe lang en met welke middelen.[64]

Uit het bovenstaande volgt dat uit de overeenkomst moet blijken wat de doeleinden van en de middelen voor de verwerking van persoonsgegevens zijn, welke soort gegevens wordt verwerkt, de duur van de opslag van de gegevens, het gebruik van de gegevens, alsmede eventuele verstrekking aan derden. Maar ook in welke mate de bewerker zeggenschap heeft, dat wil zeggen, in welke mate hij de details van de verwerkingswijze van persoonsgegevens kan bepalen. Dergelijke belangrijke elementen van de gegevensverwerking dienen in de bewerkersovereenkomst voldoende gedetailleerd te zijn opgenomen. In ieder geval zodanig dat de bewerker daadwerkelijk op instructie van de verantwoordelijke kan handelen en de verantwoordelijke daadwerkelijk toe kan zien op de feitelijke naleving daarvan.

De bewerkersovereenkomst dient eveneens te voorzien in een uitwerking van de wijze waarop de verantwoordelijke toe kan zien op de naleving van de overeengekomen waarborgen, als bedoeld in artikel 13 van de Wbp (passende technische en organisatorische maatregelen) (artikel 14, derde lid, onder b, van de Wbp).

Indien de bewerker is gevestigd in een andere lidstaat van de Europese Unie, is het recht van het land van vestiging van de bewerker van toepassing.[65] De verantwoordelijke draagt dan zorg dat de bewerker dat recht nakomt. De overeenkomst dient hiervan blijk te geven, doordat dit in de overeenkomst is geregeld.[66] Indien de opdrachtgever daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan subbewerkers. De bewerker dient dan wel contractueel verzekerd te hebben dat de subbewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt.[67] De

[62] De strekking van de bepaling is te voorkomen dat bij eventuele tekortkomingen in de gegevensverwerking verantwoordelijke en bewerker zich wat betreft hun verantwoordelijkheid achter elkaar zouden kunnen verschuilen. Idem, p. 99.
[63] Idem.
[64] Idem, p. 57.
[65] Idem, p. 100.
[66] Indien de bewerker is gevestigd in een land buiten de Europese Unie (EU), is er sprake van doorgifte van persoonsgegevens. Het uitgangspunt is dat de doorgifte van persoonsgegevens naar een land buiten de EU slechts mogelijk is, indien dat andere land voldoende bescherming biedt (artikel 76 Wbp). Wanneer een land buiten de EU onvoldoende bescherming biedt, is verkeer van persoonsgegevens niet uitgesloten, doch onderworpen aan aanvullende regels (artikel 77 Wbp). Naleving van het bepaalde in artikel 76 e.v. van de Wbp (doorgifte) valt buiten de scope van dit onderzoek door het CBP.
[67] Zie Kamerstukken II 1997-1998, 25 892, nr. 3, p. 63.

verantwoordelijke dient met het subbewerkerschap uitdrukkelijk te hebben ingestemd. Uit de overeenkomst tussen de verantwoordelijke en de bewerker dient dit te blijken.[68]

2.1.5 Informatieplicht

Artikel 33, eerste en tweede lid, van de Wbp bepaalt:
1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.

Artikel 34, eerste en tweede lid, van de Wbp bepaalt: *indien persoonsgegevens worden verkregen op een andere wijze dan bij de betrokkene, de verantwoordelijke de betrokkene zijn identiteit en de doeleinden van de verwerking, mededeelt, tenzij de betrokkene daarvan reeds op de hoogte is:*
a. op het moment van vastlegging van hem betreffende gegevens, of
b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen, tenzij de betrokkene daarvan reeds op de hoogte is (artikel 33, derde lid, en artikel 34, derde jo. eerste lid, van de Wbp).

Artikel 33 van de Wbp beschrijft de situatie dat de gegevens worden verkregen bij de betrokkene zelf, bijvoorbeeld wanneer hij aan de hand van een formulier gegevens over zichzelf moet invullen voor een bepaald doel.[69]

Artikel 34 van de Wbp regelt een informatieplicht voor de situatie dat de persoonsgegevens op een andere wijze worden verkregen dan bij de betrokkene, dus buiten de betrokkene om, hetzij bij derden, hetzij door eigen observatie, bijvoorbeeld naar aanleiding van het gebruik van een netwerk in beheer van de verantwoordelijke.[70]

Deze bepalingen vormen een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing'.[71] De verplichting van de verantwoordelijke om op eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om het gegevensverkeer transparant te maken.[72] De betrokkene is daardoor in staat

[68] Idem.
[69] Idem, p. 149.
[70] Idem, p. 149-150.
[71] Idem, p. 149.
[72] Idem.

te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.[73]

Artikel 33 en 34 van de Wbp gaan er vanuit dat er geen onderzoeksplicht van de betrokkene is.[74]

Uit de wetsgeschiedenis bij de Wbp volgt dat de ratio van de informatieverplichting is dat betrokkene in staat wordt gesteld te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.[75] De informatie moet de betrokkene voldoende houvast bieden om te kunnen voorzien wat er met zijn gegevens gebeurt.[76]

Artikel 11.7a, eerste lid, onder a, van de Tw bepaalt dat eenieder die gegevens wil uitlezen van of gegevens wil opslaan in de randapparatuur van een gebruiker *de gebruiker duidelijke en volledige informatie* [dient, toevoeging door het CBP] *te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan.*

De informatieverplichtingen uit hoofde van de Wbp, als hierboven weergegeven, zijn derhalve ook van toepassing met betrekking tot het uitlezen en plaatsen van informatie op randapparatuur van gebruikers.

2.1.6 Grondslag

Voor het verwerken van persoonsgegevens is een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8 van de Wbp.

Artikel 8, aanhef en onder a, b, c en f, van de Wbp, bepaalt, voor zover voor dit onderzoek van belang: *persoonsgegevens mogen slechts worden verwerkt indien:*
a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is; (…)

[73] Idem.
[74] Idem, p. 150.
[75] Idem, p. 149.
[76] Zie ook Kamerstukken II 1998/99, 25 892, nr. 6, p. 17: "Daar waar normaal commercieel gebruik van persoonsgegevens is toegestaan, zal de betrokkene in beginsel wel op de hoogte moeten worden gesteld van het doel waarvoor de gegevens worden verwerkt. Daarbij kan de verantwoordelijke niet volstaan met de mededeling dat gegevens in abstracto worden verwerkt voor commerciële doeleinden: dit is te weinig specifiek. Het biedt de betrokkene onvoldoende houvast om te kunnen voorzien wat er met zijn gegevens gebeurt. De betrokkene zal adequaat moeten worden geïnformeerd omtrent het concrete doel van de gegevensverwerking als toetsingskader voor zorgvuldig gebruik."

f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Ondubbelzinnige toestemming

Ten aanzien van de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp), geldt het volgende.

Van toestemming is slechts sprake indien deze 'vrij', 'specifiek' en 'geïnformeerd' is (artikel 1, aanhef en onder i, van de Wbp). 'Vrij' betekent dat de betrokkene in vrijheid zijn wil moet kunnen uiten.[77] 'Specifiek' betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).[78] 'Geïnformeerd' betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.[79]

Van *ondubbelzinnige* toestemming is slechts sprake indien bij de verantwoordelijke elke twijfel is uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.[80] 'Ondubbelzinnig' betekent dat de verantwoordelijke niet mag uitgaan van toestemming indien de betrokkene geen opmerkingen maakt over de gegevensverwerking (oftewel: bij 'toestemming' die wordt geacht voort te vloeien uit het uitblijven van actie of het stilzwijgen van de betrokkene).[81]

In de wetsgeschiedenis bij de Wbp is daarover opgemerkt:

> *"Als voorbeeld noem ik algemene voorwaarden die van toepassing zijn op het sluiten van een overeenkomst. Indien in dergelijke voorwaarden wordt bepaald welke gegevens er voor welk doel en door wie verwerkt worden, wil dat nog niet automatisch zeggen dat betrokkene daartoe ondubbelzinnig zijn toestemming heeft gegeven, enkel omdat hij de betreffende overeenkomst heeft ondertekend."*[82]

In het advies van de Artikel 29-werkgroep is over 'ondubbelzinnige toestemming' verder aangegeven:

---

[77] Idem, p. 65.

[78] Idem. In het advies van de Artikel 29-werkgroep is daarover opgemerkt: "Een algemene toestemming zonder dat precies is aangegeven wat het doel is van de verwerking waarmee de betrokkene instemt, voldoet niet aan dit vereiste. Dat betekent dat de informatie over het doel van de verwerking niet in de algemene voorwaarden moet worden opgenomen, maar in een aparte toestemmingsclausule." Artikel 29-werkgroep WP 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 40. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_nl.pdf.

[79] Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.

[80] Idem, p. 80.

[81] Idem, p. 66 en 67. Zie ook Artikel 29-werkgroep WP 187, Advies 15/2011 over de definitie van "toestemming", p. 28 en 41.

[82] Handelingen I 1999/2000, 34, p. 1632. Vgl. ook HvJ EU van 19 juli 2012, zaak C-112/11 (ebookers.com), r.o. 16 en HvJ EU van 9 november 2010, zaaknummers C-92/09 en C-93/09.

"Een "toestemming" die wordt geacht voort te vloeien uit het uitblijven van actie of het stilzwijgen van de betrokkene is normaal gesproken niet rechtsgeldig, zeker niet in een onlineomgeving. Dit speelt met name wanneer "toestemming" wordt gegeven via standaardconfiguratie-instellingen die de betrokkene moet wijzigen als hij niet wil dat zijn gegevens worden verwerkt. Dit is bijvoorbeeld het geval bij vooraf aangevinkte vakjes of bij browsers die standaard zo zijn ingesteld dat ze cookies accepteren."[83]

Als de toestemming niet aan bovenstaande vereisten voldoet is zij nietig.[84]

Ten aanzien van het plaatsen en uitlezen van informatie op eindapparatuur van gebruikers geeft artikel 11.7a van de Tw een nadere begrenzing/inperking van de mogelijke grondslagen als opgesomd in artikel 8 van de Wbp die voor de verwerking van persoonsgegevens mogelijk in aanmerking komen. Op grond van de Tw mogen dergelijke handelingen alleen na voorafgaande toestemming van de gebruikers.

Artikel 11.7a van de Tw luidt, voor zover voor dit onderzoek van belang:
1. Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker:
a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en
b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling.
Een handeling als bedoeld in de aanhef, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren voor commerciële, charitatieve of ideële doeleinden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.
(…)
3. Het bepaalde in het eerste en tweede lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:
a. de communicatie over een elektronisch communicatienetwerk uit te voeren, of
b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.[85]

[83] Artikel 29-werkgroep WP 187, Advies 15/2011 over de definitie van "toestemming", p. 41.
[84] Kamerstukken II 1997/98, 25 892, nr. 3, p. 67.
[85] Op 20 mei 2013 is een conceptwetsvoorstel tot aanpassing van artikel 11.7a Tw in openbare consultatie gegaan. Zie: http://www.internetconsultatie.nl/cookiebepaling (de consultatie loopt tot 1 juli 2013). Doel van de voorgestelde aanpassing is dat niet meer hoeft te worden geïnformeerd en geen toestemming meer hoeft te worden gevraagd als met het plaatsen of lezen van een cookie informatie wordt verkregen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de internetter. Daaronder

Toestemming van een gebruiker is gedefinieerd in artikel 11.1, aanhef en onder g, van de Tw en omvat 'vrije', 'specifieke' en 'geïnformeerde' toestemming (artikel 1, aanhef en onder i, van de Wbp).

Uitvoering van een overeenkomst

Ten aanzien van de grondslag uitvoering van een overeenkomst (artikel 8, aanhef en onder b, van de Wbp) geldt het volgende.

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is om contractuele verplichting(en) na te komen.[86] Daarbij geldt als voorwaarde dat het moet gaan om een overeenkomst waarbij de betrokkene partij is[87] en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (dat wil zeggen: als de overeenkomst niet goed kan worden uitgevoerd zonder de persoonsgegevens).[88] De uitgever van een krant mag bijvoorbeeld de persoonsgegevens van zijn abonnees verwerken omdat dat noodzakelijk is om de krant te kunnen bezorgen[89] (zonder NAW-gegevens van de betrokkene kan bezorging niet plaatsvinden). De verwerking kan niet worden gebaseerd op deze grondslag als de verwerking nuttig zou zijn of de uitvoering van een overeenkomst zou vergemakkelijken, maar niet echt noodzakelijk is aangezien er een manier bestaat om de overeenkomst uit te voeren zonder de persoonsgegevens (proportionaliteits- en subsidiariteitstoets).[90] De grondslag is strikt beperkt tot de gegevens die voor de uitvoering van de overeenkomst noodzakelijk zijn.

Het EHRM overweegt in zijn arrest van 25 maart 1983 over het begrip 'noodzakelijk': *"(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (…)."*[91]

---

vallen volgens dit conceptwetsvoorstel analytische cookies, mits het bedrijf dat zijn gebruiksgegevens uit analytic cookies deelt met een derde in een (bewerkers-) overeenkomst duidelijk afspreekt met de derde dat ook hij de informatie niet zal gebruiken op een manier die meer dan geringe gevolgen heeft voor de privacy van de internetgebruiker wiens gegevens het betreft. Toelichting bij Concept wetsvoorstel ten behoeve van internetconsultatie, p. 8.

[86] Kamerstukken II 1997/98, 25 892, nr. 3, p. 80.

[87] Idem. "Achterliggende gedachte is dat de betrokkene zelf in principe kan overzien met welke verwerkingen hij heeft rekening te houden en de mogelijkheid heeft objectief vast te stellen welke verwerkingen in dit kader toelaatbaar zijn. " CBP 31 juli 2001, z2001-0179.

[88] Kamerstukken II 1997/98, 25 892, nr. 3, p. 81.

[89] Handleiding voor verwerkers van persoonsgegevens. Wet bescherming persoonsgegevens, Ministerie van Justitie, Den Haag: 2002, p. 22.

[90] Zie ook HR 9 september 2011, LJN BQ8097 over onder andere het proportionaliteits- en subsidiariteitsvereiste bij de grondslagen, zoals bedoeld in artikel 8, aanhef en onder a tot en met e, van de Wbp. De inbreuk op de belangen van de bij de verwerking betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel (proportionaliteit) en het doel waarvoor de persoonsgegevens worden verwerkt mag in redelijkheid niet op een andere, voor de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwezenlijkt (subsidiariteit).

[91] EHRM 25 maart 1983, nr. 97 (Silver & Others v. United Kingdom).

Als aanvullende, niet-essentiële gegevens worden verwerkt is deze grondslag niet van toepassing. Anders gezegd: er moet een rechtvaardiging voor de verwerking aanwezig zijn *in de relatie tot de specifieke individuele betrokkene*.[92] Dat betekent dat de grondslag alleen kan worden toegepast als de verantwoordelijke de overeenkomst met deze betrokkene niet goed kan uitvoeren zonder zijn specifieke, individuele persoonsgegevens.

Wettelijke verplichting

Ten aanzien van de grondslag wettelijke plicht (artikel 8, aanhef en onder c, van de Wbp), geldt het volgende.

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is om een wettelijke verplichting na te komen.[93] Daarbij geldt als voorwaarde dat het moet gaan om een verplichting, opgenomen in een wettelijke bepaling, die op de verantwoordelijke rust en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (zonder verwerking van de persoonsgegevens moet het uitvoeren van de wettelijke verplichting redelijkerwijs niet goed mogelijk zijn; proportionaliteits- en subsidiariteitstoets).[94] Anders gezegd: er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.[95] Daarbij moet onder andere worden gelet op de aard van de in het geding zijnde taak en de aard van de betrokken persoonsgegevens.[96] De taak een wettelijke verplichting uit te voeren rechtvaardigt niet elke gegevensverwerking. Als aanvullende, niet-essentiële gegevens worden verwerkt is deze grondslag niet van toepassing. [97] De wettelijke verplichting moet voldoende specifiek zijn om een verplichting om persoonsgegevens te verwerken aan te nemen. De verplichting behoeft geen expliciete opdracht tot gegevensverwerking te bevatten.[98]

Gerechtvaardigd belang

Ten aanzien van de grondslag gerechtvaardigd belang (artikel 8, aanhef en onder f, van de Wbp) geldt het volgende.

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke (bijvoorbeeld om zijn reguliere bedrijfsactiviteiten te kunnen verrichten[99]) of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de

[92] Vgl. Kamerstukken II 1998/99, 25 892, nr. 6, p. 34: "Dat betekent dat in de regel een rechtvaardiging voor gegevensverwerking aanwijsbaar moet zijn in de individuele persoon over wie gegevens worden vergaard."
[93] De wettelijke regeling waarmee de verplichting in het leven wordt geroepen, moet uiteraard wel voldoen aan artikel 8 van het EVRM. Kamerstukken II 1997/98, 25 892, nr. 3, p. 83.
[94] Idem, p. 82-83. Een verwerking die uitsluitend dient ter uitvoering van een wettelijk recht valt hier buiten.
[95] Idem, p. 82.
[96] Idem, p. 83.
[97] Idem.
[98] Idem.
[99] Idem, p. 86.

persoonlijke levenssfeer, prevaleert. Deze grondslag kan worden toegepast indien de verwerking noodzakelijk is (proportionaliteitstoets: de inbreuk op de belangen van de bij de verwerking betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel) en het doeleinde niet anderszins of met minder ingrijpende middelen kan worden bereikt (subsidiariteitstoets).[100]

In aanvulling op deze eerste afweging (noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke), waarbij mogelijk de belangen van de betrokkene als onderdeel van een veelheid van belangen al onder ogen zijn gezien, is er nog een tweede toets.[101] Deze tweede toets (privacytoets) vergt een nadere afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. In het geval dat het belang van de betrokkene op bescherming van zijn persoonlijke levenssfeer doorslaggevend is, dient de verantwoordelijke af te zien van de gegevensverwerking.[102]

2.2 Feitelijke bevindingen

2.2.1 TP Vision

TP Vision, gevestigd te Amsterdam en kantoorhoudende te Amsterdam en Eindhoven, is opgericht op 22 juni 2011 en ingeschreven bij de Kamer van Koophandel onder nummer 53045394. De doelomschrijving van TP Vision is: *"De marketing en in- en verkoop van en anderszins handeldrijven in en service verlenen aan elektrische, elektronische, mechanische en andere producten en systemen, met name televisies en daaraan verwante artikelen en systemen."* TP Vision houdt zich bezig met het design, de productie, de distributie, marketing en verkoop van de Philips smart tv's. Philips produceert sinds 2009 smart tv's. Op 2 april 2012 heeft Philips haar televisie-divisie verkocht aan TPV Technology Limited, gevestigd te Hong Kong.[103] TP Vision Holding B.V., de moedermaatschappij van TP Vision Nederland B.V., is een joint venture van Koninklijke Philips Electronics N.V. en TPV Technology Limited. Philips bezit 30% van de aandelen, TPV Technology Limited bezit 70% van de aandelen in de joint venture.[104]

TP Vision heeft verklaard dat er in Nederland sinds 2009 1 tot 1,2 miljoen Philips smart tv's zijn verkocht. Op de helft van deze toestellen is ooit de internetfunctionaliteit gebruikt. Op naar schatting 350.000 tot 400.000 van deze

[100] Vgl. de proportionaliteits- en subsidiariteitstoets uit artikel 8 EVRM. Kamerstukken II 1997/98, 25 892, nr. 3, p. 80. Zie ook idem, p. 8 en idem, nr. 92c, p. 6.
[101] Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.
[102] Idem.
[103] Persbericht Philips, Philips en TPV kondigen start tv-joint venture TP Vision aan, 2 april 2012, URL: http://www.newscenter.philips.com/nl_nl/standard/about/news/press/20120402-TP-Vision.wpd. Zie ook het zakelijk profiel van TP Vision Holding B.V., URL: http://www.tpvholdings.com/html/corp_profile.php
[104] Idem.

toestellen wordt de internetfunctionaliteit actief gebruikt, dat wil zeggen dat een gebruiker ten minste één keer per maand een app gebruikt.[105]

TP Vision had de verwerking van persoonsgegevens, voor zover voor dit onderzoek van belang, bij aanvang van dit onderzoek niet gemeld bij het CBP. Naar aanleiding van het onderzoek heeft TP Vision op 16 oktober 2012 gegevensverwerkingen via het smart tv-portal gemeld bij het CBP. Deze melding heeft nummer m1519483. In de melding zijn, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

Verwerking van gegevens via het SmartTV Portal

Het onderhouden en het leveren van de SmartTV Portal.
Het verbeteren van de open Internet browsing ervaring via de Portal.
Het autoriseren en verwerken van betaaltransacties via een SmartTV Payment account.
Het verbeteren van de advertentie ervaring: TPVN gebruikt gegevens betreffende advertentie views en kliks op advertenties om de advertentie ervaring van consumenten in het kader van de SmartTV Portal te verbeteren.
Kijkaanbevelingen voor TVs: Indien en voor zover een consument binnen de Portal "gepersonaliseerde aanbevelingen" heeft aangezet gebruikt TPVN gegevens betreffende het kijkgedrag om kijkaanbevelingen te doen.
Het verlenen van korting content of gratis content door applicatie aanbieders aan consumenten.
Gebruik ten behoeve van authenticatie van TVs door applicatie aanbieders.
Het verstrekken aan politie en justitie op grond van een bevoegd gegeven last of vordering of op basis van een andere wettelijke verplichting.
Het optimaliseren van de gebruikerservaring van de Portal voor consumenten.

In de melding geeft TP Vision aan de volgende persoonsgegevens te verwerken:

Uniek nummer voor een consument/eigenaar van een TV (Consumer ID)
Uniek nummer voor een mobiel apparaat (Mobile Device ID)
IP nummer (in server logs en data base entries)
Advertentie kijk en klik gedrag per Device-ID
URL's die in de browser op een TV worden ingegeven
Kijkgedrag
Betaaltransactiegegevens
Applicatie klik gedrag
TV specifieke informatie zoals typenummer en geconfigureerde taal/land
Uniek netwerk nummer voor een TV (Device-ID)

TP Vision geeft in de melding aan géén bijzondere persoonsgegevens te verwerken.[106]

[105] Verklaring TP Vision tijdens het onderzoek ter plaatse, bevestigd door het CBP per brief van 16 oktober 2012.

In de melding geeft TP Vision aan gebruik te maken van vier bewerkers, namelijk IBM Nederland B.V. (hierna: IBM), Gracenote GmbH uit Duitsland (hierna: Gracenote), MPP Global Solutions Ltd uit het Verenigd Koninkrijk (hierna: MPP Global) en Philips Electronics Nederland B.V. (hierna: Philips).

2.2.2 Gegevensverwerking

Op een Philips smart tv zoals die in Nederland wordt verkocht zijn de volgende internetfunctionaliteiten beschikbaar. Via de ingebouwde Opera-browser kunnen gebruikers websites bekijken. Gebruikers kunnen daarnaast een groot aantal apps gebruiken via de *App Gallery*.[107]

> De apps zijn web apps, dat wil zeggen, HTML pagina's die gehost zijn bij app ontwikkelaars. Gebruikers kunnen niet zelf apps op het toestel installeren, maar gebruiken feitelijk hyperlinks naar webpagina's die geschikt zijn gemaakt voor gebruik op een smart tv. De enige app die echt op het toestel zelf is geïnstalleerd, is YouTube. TP Vision heeft geen API (*application programming interface*)[108] waarmee ontwikkelaars zelfstandig toegang zouden kunnen krijgen tot gegevens in of over het toestel.[109]

Op het toestel is een online tv-gids beschikbaar (IP-EPG) en een onlinedienst die op basis van het kijkgedrag aanbevelingen doet (*recommender*). De gebruiker kan (via de apps) specifieke films of series bekijken (*video on demand*) en eventueel opnames maken op een apart aan te sluiten harde schijf. Gebruikers kunnen voor content betalen via het *payment service portal*. Daarnaast kan het toestel bestuurd worden via een meegeleverde afstandsbedieningsapp op smartphones of tablets. Bij het toestel worden apart een camera en een microfoon geleverd.

Samenwerking met andere bedrijven

TP Vision werkt samen met zes bedrijven om de onlinediensten te bieden. Technisch gezien worden de onlinediensten geleverd via twee aparte portals, een 'device portal' en een 'service portal'. Het device portal zorgt voor technische herkenning en aanmelding van het toestel. Via het device portal kan de gebruiker zich registreren. Het device portal wordt beheerd door Philips Electronics Nederland B.V.[110]
De via het device portal verzamelde registratiegegevens worden verwerkt door Philips Consumer Lifestyle B.V.[111]

---

[106] Naleving van het bepaalde in artikel 16 e.v. van de Wbp (bijzondere persoonsgegevens) valt buiten de scope van dit onderzoek door het CBP.
[107] Presentatie TP Vision tijdens het onderzoek ter plaatse, p. 12. Het Philips Smart TV Partner Portal bevat "1500 Apps live per today". Daarin begrepen zijn 250 ‘premium apps’ en 50 ‘catch-up tv apps’ (uitzending gemist).
[108] Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel (meestal in de vorm van bibliotheken). Bron: Wikipedia, http://nl.wikipedia.org/wiki/Application_programming_interface (URL laatst bezocht op 15 november 2012).
[109] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 11.
[110] Idem, par. 16: "(…) de Device portal wordt beheerd door Philips Electronics Nederland B.V. (…)"

Het service portal is eigendom van TP Vision en wordt beheerd door IBM.[112] Via het service portal zijn de tv-gids, de recommender en betalingsmogelijkheden toegankelijk. De programmagegevens in de tv-gids en de recommender zijn eigendom van Gracenote en in licentie gegeven aan TP Vision.[113] De betalingsmogelijkheden worden beheerd door MPP Global.[114] Daarnaast maakt TP Vision gebruik van de diensten van Google (Google Analytics voor informatie over het gebruik van apps en het bezoek aan websites met de tv) en van Akamai (snel downloaden onlinefilms en uitzendingen).[115]

Uit de door TP Vision verstrekte datamodellen, verklaringen, de inhoud van de melding bij het CBP, het privacystatement van 12 oktober 2012, zoals herzien op 1 mei 2013 en (herziene) overeenkomsten met genoemde partijen blijkt het volgende.

TP Vision heeft verklaard geen registratiegegevens te ontvangen van **Philips**.[116] TP Vision is ook geen 'business unit' van Philips.[117] Tijdens het onderzoek ter plaatse verklaarde TP Vision dat in de overeenkomsten tussen Philips en TP Vision niet was vastgelegd dat TP Vision geen registratiegegevens kreeg van Philips.[118] Naderhand verstrekte TP Vision een handelsmerklicentieovereenkomst met Philips Consumer Lifestyle B.V.[119] waarin is bepaald dat Philips de registratiegegevens van Nederlandse houders niet zal delen met TP Vision [in de overeenkomst aangeduid als Licensee] voor het doeleinde van direct marketing van de tv's.[120] Philips stelt TP Vision wel in

---

[111] Idem, par. 3: "Consumenten die vanaf 1 april 2012 een Philips SmartTV aanschaffen worden bij het opstarten van de tv gevraagd om zich te registreren bij Club Philips. Deze registratie gegevens berusten uitsluitend bij Philips Consumer Lifestyle B.V. en worden door deze entiteit verwerkt in overeenstemming met CBP registratie 1166347."

[112] Idem, par. 16: "(…) de NetTV services and Partner Portal worden beheerd door IBM Nederland B.V. (…)"

[113] Idem, "(…) de IP-EPG Data Provider is Gracenote GmbH (…)"

[114] Idem, "(…) de PSP Portal wordt beheerd door MPP Global Solutions (…)"

[115] Verklaringen TP Vision over Google en Akamai tijdens onderzoek ter plaatse, zoals bevestigd door het CBP bij brief van 16 oktober 2012. Beide partijen worden tevens genoemd in het TP Vision smart tv privacy statement van 12 oktober 2012, zoals herzien op 1 mei 2013.

[116] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 6: "Alle informatie betreffende Club Philips berust uitsluitend bij Philips Consumer Lifestyle B.V. en wordt niet gedeeld met TPVN."

[117] Omdat Philips een aandeel heeft van 30% en geen controlling interest valt TP Vision ook niet onder de BCR (Binding Corporate Rules) die Philips heeft vastgesteld ten aanzien van de gegevensverwerking door haarzelf en dochtermaatschappijen. Deze BCR zijn 14 augustus 2012 geautoriseerd door het CBP namens alle privacytoezichthouders in de EU. Uit de BCR blijkt dat de BCR alleen van toepassing zijn op bedrijven waarin Philips een meerderheidsbelang heeft in de aandelen, dan wel meer dan 50% van de stemmen heeft bij aandeelhoudersvergaderingen, de bevoegdheid om een meerderheid van bestuurders te benoemen of op andere wijzen de activiteiten bepaalt van het andere bedrijf.

[118] Verklaring TP Vision tijdens het onderzoek ter plaatse, zoals door het CBP bevestigd bij brief van 16 oktober 2012.

[119] Trademark License Agreement tussen Philips Consumer Lifestyle B.V. en TP Vision Holding B.V., gedateerd 1 november 2011, verstrekt door TP Vision bij fax van 18 oktober 2012.

[120] Dit is bepaald in Clausule J (Relevant Clause on CRM / Direct Marketing) in bovengenoemde License Agreement.

staat om deel te nemen aan Philips directmarketingcampagnes *"for example covering products in direct marketing e-mail news-letters from Philips sent to consumers that registered for Philips products."* En: *"Also dedicated e-mail campaigns related to Products can be executed by Philips on request and at the expense of Licensee, for example, informing registered consumers about a major firmware upgrade."*[121] TP Vision heeft verklaard in dat geval geen toegang te krijgen tot de database. Philips voert de verzending uit, of laat die uitvoeren.[122]

De overeenkomst bevat tevens een uitzondering voor eigen marktonderzoek door TP Vision: *"Licensee will also be allowed to get access to the registration data for the purpose of internal market research only, e.g. to make consumer profiles. In such case Licensee will enter into a data processing agreement with Philips, in which Licensee warrants to take the necessary measures to protect the data and ensure consumer privacy laws are respected."*[123] Aanvullend heeft TP Vision verklaard dat het nog niet is voorgekomen dat Philips de gegevens in de database met TP Vision heeft gedeeld voor interne onderzoeksdoeleinden en dat dit voorlopig ook nog niet het geval zal zijn.[124] Om die reden heeft TP Vision ook (nog) geen bewerkersovereenkomst gesloten met Philips. "*Mochten de plannen met betrekking tot dergelijk gebruik wijzigen, dan zullen TP Vision en Philips eerst een bewerkersovereenkomst tekenen.*"[125]

In 2008 heeft Philips een overeenkomst gesloten met de rechtsvoorganger van **Gracenote** voor de levering van tv-gidsinformatie, de IP-EPG.[126] Bij die overeenkomst hoort een gebruikersovereenkomst (Terms of Use - TOU)[127], die de rechten en plichten van de leverancier en gebruiker beschrijft ten aanzien van de levering van programma-informatie. Volgens de overeenkomst dient Philips ervoor te zorgen dat gebruikers van de dienst akkoord gaan met deze gebruikersovereenkomst.[128]

In een aparte overeenkomst tussen TP Vision en Gracenote wordt beschreven wat voor recommenderdiensten Gracenote is overeengekomen te gaan leveren, in aanvulling op het aanleveren van de programma-informatie.[129] Dit zijn onder meer: [VERTROUWELIJK]. Genoemde overeenkomsten bevatten geen informatie over de verwerking van (persoons-)gegevens.

Op 18 december 2012 heeft TP Vision een conceptovereenkomst (Data Processor Agreement) verstuurd aan Gracenote. Bij e-mail van 5 februari 2013 heeft TP Vision aan het CBP de definitief vastgestelde tekst van de overeenkomst verstrekt. TP Vision

---

[121] Idem.
[122] Brief TP Vision van 8 mei 2013, p. 3.
[123] Clausule J (Relevant Clause on CRM / Direct Marketing).
[124] Brief TP Vision van 8 mei 2013, p. 3.
[125] Idem
[126] Agreement between tvtv Services and Philips Consumer Lifestyle, 17 december 2008.
[127] Idem, Annex 7 TOU General Terms and Conditions, gedateerd oktober 2006.
[128] Agreement between tvtv Services and Philips Consumer Lifestyle B.V., paragraaf 6.2: "(…) Philips further undertakes that prior to using the tvtv data each end user declares to have read and bindingly accepted the TOU by pushing the continue button. (…)"
[129] Professional Services Agreement - TP Vision Recommender Phase 3, Statement of Work #5, 27 juli 2012.

heeft daarbij verklaard dat de tekst was gebaseerd op de EU-modelbepalingen voor een verantwoordelijke-bewerker en dat de bepalingen niet waren gewijzigd (*Standard Contractual Clauses*).[130] Een week later heeft TP Vision een nieuwe versie van de overeenkomst aan het CBP toegezonden, die volgens TP Vision definitief en volledig ondertekend zou zijn.[131] Dit bleek echter niet het geval te zijn.

Bij brief van 8 mei 2013 heeft TP Vision het CBP een (tweede) door partijen ondertekende Data Processor Agreement toegestuurd, gedateerd op 6 mei 2013. Deze tweede overeenkomst bevat (onder meer) de verplichtingen die Gracenote als bewerker op zich neemt naar Nederlands recht. De overeenkomst heeft naar zijn aard betrekking op de gegevensverwerking en bevat bepalingen over technische en organisatorische beveiligingsmaatregelen (onder meer in Annex 2). Daarnaast zijn bepalingen opgenomen over de mate van zeggenschap van de bewerker, het gebruik van de gegevens, audit, opslag en bewaartermijnen van de gegevens. De overeenkomst bevat de volgende doelomschrijving: "*The Recommendation-Related Information is used by GraceNote to create recommendations for Consumers.*"[132] In Annex 1 is een lijst opgenomen met de soorten gegevens die worden verwerkt. Dit zijn: IP-adressen (bewaartermijn 30 dagen) en Device ID, "*the electronic program guide viewing history for the particular Device; catch-up TV shows that are selected on the particular Device; and Video-on-demand items purchased via the particular Device*" (bewaartermijn drie maanden).

Uit de Agreement blijkt dat naast deze bewerkersovereenkomst óók de standard contractual clauses blijven gelden (voor doorgifte van gegevens naar de VS): "*for clarity, the Standard Contractual Clauses (Processors) Agreement signed by GraceNote, Inc. and TPVN on or about January 31, 2013, shall be deemed amended hereby to reflect the foregoing.*"[133]

Op 1 december 2008 hebben Philips en **IBM** een uitgebreide overeenkomst gesloten met betrekking tot het service portal.[134] Deze overeenkomst bevat een korte paragraaf over persoonsgegevens, waarin IBM alleen aangeeft met betrekking tot de verwerking en beveiliging van persoonsgegevens te handelen op instructies van Philips.[135] Op 25 januari 2012 heeft Philips alle rechten en verplichtingen overgedragen aan TP Vision B.V. IBM heeft deze overdracht geaccepteerd en (mede) ondertekend.[136]

---

[130] E-mail TP Vision aan het CBP van 5 februari 2013.
[131] E-mail TP Vision aan het CBP van 13 februari 2013.
[132] Onderliggende stukken bevatten meer gedetailleerde opdrachten aan Gracenote, met name Statement of Work #5 van 27 juli 2012.
[133] Annex 1 List of Data Types, p. 6 van de Data Processor Agreement tussen TP Vision Netherlands B.V. en Gracenote GmbH, van 6 mei 2013.
[134] IBM Full Service Framework Agreement between IBM Nederland B.V. and Philips Consumer Lifestyle B.V., gedateerd 1 december 2008 (Engelstalig). Aan het CBP verstrekt door TP Vision op 23 oktober 2012. Blijkens de tekst is de overeenkomst een aanvulling op een eerdere Master Agreement van 15 januari 2005.
[135] Idem, paragraaf 11.16 Data Protection, p. 53.
[136] Brief Philips Consumer Lifestyle B.V. aan IBM Nederland B.V. van 25 januari 2012, ondertekend door IBM in maart 2012. De brief spreekt over overdracht aan TP Vision B.V. en is mede ondertekend door TP Vision Holding B.V.

Op 13 juli 2012 hebben TP Vision en IBM een Services Agreement gesloten.[137] Deze overeenkomst bevat bepalingen over de diensten die IBM levert aan TP Vision in het kader van het ter beschikking stellen van een cloudplatform.

Aan de schriftelijke beantwoording van de vragen van het CBP heeft TP Vision als bijlage een conceptaanvulling op de overeenkomst met IBM toegevoegd. Op 18 december 2012 heeft TP Vision een conceptovereenkomst (Data Processor Agreement), in overeenstemming met het eerder toegestuurde model,[138] verstuurd aan IBM. Bij brief van 8 mei 2013 heeft TP Vision het CBP een door partijen ondertekende Data Processor Agreement toegestuurd, gedateerd op 6 mei 2013.

De overeenkomst bevat (onder meer) verplichtingen die IBM als bewerker op zich neemt naar Nederlands recht. De overeenkomst heeft naar zijn aard betrekking op de gegevensverwerking, bevat bepalingen over technische en organisatorische beveiligingsmaatregelen (onder meer in Annex 2). Daarnaast zijn bepalingen opgenomen over de mate van zeggenschap van de bewerker, het gebruik van de gegevens, audit en bewaartermijnen van de gegevens. De algemene doelomschrijving (*fulfilment and maintenance of a part of platform of the SMART TV Portal*) is gedetailleerd uitgewerkt in onderliggende stukken.[139]

Annex 1 bevat een lijst met de soorten gegevens die worden verwerkt. Dit zijn: Consumer ID, Device ID en IP-adres (bewaartermijn: *permanently*). Onder 'Usage Information' wordt beschreven:
"*-Information on notifications viewed/accepted (including opt-in/opt-out choices);*
-Information on locked categories (including were PIN codes are required);
-Information on URL history (limited to four (4) values) and bookmarks;
-Information on app installation, app activation, and app positioning on the screen"
(bewaartermijn permanent, *until the user of the television clears or deletes the values*)"

Bij brief van 8 mei 2013 heeft TP Vision aangegeven dat "*op korte termijn een additionele overeenkomst in lijn met de 'Standard Contractual Clauses' worden ondertekend, omdat gebleken is dat data eventueel ook naar servers buiten de EU worden verzonden.*"[140] TP Vision heeft telefonisch aangegeven deze overeenkomst uiterlijk eind juni 2013 te zullen toesturen aan het CBP.[141]

---

[137] Global Process Services Consumer Electronics Service Delivery Platform Services Agreement van 13 juli 2012, ondertekend door TP Vision Netherlands B.V. en IBM Nederland B.V.
[138] Bijlage A bij de schriftelijke beantwoording van de vragen van het CBP door TP Vision van 16 januari 2013.
[139] Onder andere in Global Process Services Consumer Electronics Service Delivery Platform Services Agreement van 13 juli 2012, ondertekend door TP Vision Netherlands B.V. en IBM Nederland B.V. en IBM Consumer Electronics - Cloud Service Delivery Platform TP Vision NetTV Service Portal Architecture Overview - Privacy Perspective Version 03, oktober 2012.
[140] Brief TP Vision van 8 mei 2013, p. 1
[141] Telefonische inlichting TP Vision, 5 juni 2013. Naleving van het bepaalde in artikel 76 e.v. van de Wbp (doorgifte) valt buiten de scope van dit onderzoek door het CBP.

In oktober 2012 heeft IBM aan TP Vision een overzicht geleverd van de architectuur van het service portal vanuit privacyperspectief[142] en een datamodel.[143] Dit document beschrijft en visualiseert het datamodel van het service portal. IBM schrijft dat via het service portal geen (bijzondere) persoonsgegevens worden verwerkt. Wel verwerkt het service portal twee unieke nummers (Consumer ID en Device ID) waarmee volgens IBM "*a consumer, or a particular consumer electronics device can be uniquely identified within its datamodel and technical mechanisms* (…)."[144] Via de database van het Service Portal, waarin de combinatie van Consumer ID met Device ID als koppelvlak dient[145], heeft TP Vision toegang tot (door IBM zelf gemaakte) statistieken op individueel niveau over appgebruik en websitebezoek, in de vorm van een overzicht van individueel geïnstalleerde apps, hun volgorde op het scherm en (de frequentie van) het gebruik van die apps, het gebruik van bookmarks en de laatste vier door de gebruiker zelf ingevoerde URL's.

Philips sloot in 2011 tevens een overeenkomst met **MPP Global** om betalingsdiensten te gaan leveren via het service portal, zowel pay per view als abonnementsdiensten, inclusief mobiele betalingen (via de rekening van de telefoonaanbieder).[146] Blijkens een persbericht van TP Vision is de dienst eind oktober 2012 daadwerkelijk beschikbaar gekomen voor houders van een Philips smart tv in Nederland. De eerste aanbieder is Videoland, voor het online huren van films.[147]

Uit de overeenkomst tussen Philips en MPP Global, zoals overgedragen aan TP Vision, blijkt dat TP Vision via de 'Customer Management Console' van MPP Global toegang krijgt tot gegevens van klanten die zich hebben aangemeld voor betalingsdiensten. Het gaat (bij volledige registratie) om naam en adresgegevens, bankrekeningnummers en betalingsgegevens (inclusief type betaling en datum van aankoop, en ook gebruikte 'credits' en eventuele redenen van terugstorting).[148] TP Vision kan via deze console gegevens downloaden en profielen maken: "*segment the data by the fields obtained, download segments of the data defined in the Business*

[142] IBM Consumer Electronics - Cloud Service Delivery Platform TP Vision NetTV Service Portal Architecture Overview - Privacy Perspective Version 03, oktober 2012.
[143] Bijlage 4 bij de reactie van TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP.
[144] IBM Consumer Electronics - Cloud Service Delivery Platform TP Vision NetTV Service Portal Architecture Overview - Privacy Perspective Version 03, oktober 2012, p. 8.
[145] Idem, p. 14. Het gaat om de tabel 'Device_Consumer' met als toelichting: "Represents a combination of a unique device and a unique consumer. Used as a central table to link to other data that requires this combination."
[146] Philips Consumer Lifestyle B.V. and MPP Global Solutions Ltd, Framework agreement for the supply of services and payment solution inclusief annex A, Statement of Work, beide gedateerd 31 augustus 2011. Aan het CBP verstrekt door TP Vision op 23 oktober 2012.
[147] Persbericht TP Vision, 29 oktober 2012, Direct betalen op je Philips Smart TV, URL: http://www.tpvision.nl/pr/press-release/direct-betalen-op-je-philips-smart-tv/tp-vision-global. Zie ook: http://www.hdtvnieuws.nl/hdtv/philips-smart-tv-payment-20121026/.
[148] Business Requirements Definition, Philips en MPP Global Statement of Work, Schedule A van 14 juni 2011, paragraaf 6.3, behorend bij Framework agreement Philips en MPP Global. Er is ook een 'light' registratie, waarbij MPP Global van de gebruiker van de tv e-mail adres, (zelfbedachte) pincode en creditcardgegevens verzamelt..

Requirements Document in a CSV format." TP Vision kan via deze console ook e-mails en sms sturen aan klanten.[149]

Op 30 december 2012 heeft TP Vision een voorstel gedaan aan MPP Global tot het aangaan van een bewerkersovereenkomst. Partijen hebben een Data Processor Agreement ondertekend op 5 februari 2013.[150] De overeenkomst bevat (onder meer) verplichtingen die MPP Global als bewerker op zich neemt naar Engels recht. De overeenkomst heeft naar zijn aard betrekking op de gegevensverwerking, in Annex 2 zijn de te treffen technische en organisatorische beveiligingsmaatregelen opgenomen en de overeenkomst bevat bepalingen over onder meer de mate van zeggenschap van de bewerker, het gebruik van de gegevens, audit en bewaartermijn van de gegevens. In Annex 1 worden de soorten gegevens gecategoriseerd. Dit zijn: "*all data connected with a Smart TV Payment Account, included but not limited to first name family name, country of residence, e-mail address, information related to the payment instrument utilized by the Consumer (credit card number and issuer, bank account number and balance etc.), Device ID, and all payment transaction information (acquired video-on-demand and other content).*"[151]

De algemene doelomschrijving in de overeenkomst (*fulfilment and maintenance of a part of platform of the SMART TV Portal*) is nader uitgewerkt in de (onderliggende) *Outsourcing Agreement*.[152] Hierin zijn de door MPP Global te leveren diensten alsmede de wederzijdse verplichtingen van de contractpartijen nader uitgewerkt.

Via IBM maakt TP Vision gebruik van de diensten van **Akamai**. Akamai is een wereldwijd opererende clouddienst die de inhoud van druk bezochte websites tijdelijk kopieert ('*mirrort*') en ervoor zorgt dat bijvoorbeeld films en streaming media sneller bij gebruikers worden afgeleverd (via servers zo dicht mogelijk bij de gebruikers). IBM heeft in 2009 een specifieke reseller-overeenkomst met Akamai gesloten voor Nederland.[153] Onder het kopje 'Data Privacy'[154] verklaart Akamai

---

[149] Framework agreement Philips en MPP Global, Annex A, Statement of Work, paragraaf 5.1.10: "provide secure access via a username and password to a Customer Management Console enabling the Customer (dwz TP Vision, toevoeging CBP) to have an overview of the data held, segment the data by the fields obtained, download segments of the data defined in the Business Requirements Document in a CSV format and send Email and SMS text messages to all or segmented end-Users."

[150] E-mail TP Vision van 6 februari 2013, bijlage.

[151] Data Processor Agreement tussen MPP Global Solutions Ltd en TP Vision Netherlands B.V. ondertekend op 5 februari 2013.

[152] De artikelen 1.4, 3.1 en 4.1 van de overeenkomst verwijzen naar deze (onderliggende) Outsourcing Agreement. Deze overeenkomst omvat de MPP Global Framework Agreement van 31 augustus 2011 met Philips Consumer Lifestyle B.V. en een Statement of Work van dezelfde datum met dezelfde contractpartijen. TP Vision heeft deze onderliggende document toegestuurd bij brief van 8 mei 2013, als bijlagen 8 en 9. Paragraaf 4 bevat een beschrijving van de doeleinden van de dienstverlening, p. 8-9 van eerst genoemde overeenkomst.

[153] Akamai Participation Agreement The Netherlands, gedateerd 22 oktober 2009, door TP Vision aan het CBP verstrekt op 23 oktober 2012. De overeenkomst is getekend door Akamai Technologies GmbH in Berlijn, Duitsland.

[154] Idem, paragraaf 3.4, p. 4.

persoonsgegevens alleen te verwerken ten behoeve en op instructies van IBM, met dien verstande dat IBM akkoord dient te gaan met doorgifte van persoonsgegevens door Akamai buiten de EU voor zover noodzakelijk voor de dienstverlening.[155] Akamai verklaart voorts passende beveiligingsmaatregelen te treffen en alle verplichtingen na te leven die op haar rusten als bewerker, inclusief ondersteuning bij het uitoefenen van het recht van inzage door betrokkenen, het meewerken aan een audit door en op kosten van IBM en het desgevraagd teruggeven of verwijderen van alle persoonsgegevens na opzegging van de overeenkomst.

Naar aanleiding van het onderzoek heeft TP Vision aan de bewerkersovereenkomst met IBM bepalingen toegevoegd met betrekking tot subbewerkerschap. Uit de overeenkomst blijkt dat TP Vision IBM ruimte laat om delen van de verwerking uit te besteden aan subbewerkers. Meer specifiek is bepaald dat de subbewerker zich moet richten naar instructies van TP Vision en de bewerker IBM, dat de subbewerker bepaalde beveiligingsmaatregelen moet implementeren alsmede tot geheimhouding verplicht is. Daartoe zal IBM nog een specifieke overeenkomst sluiten met de betreffende subbewerker.

Ten aanzien van de dienst **Google Analytics** heeft TP Vision verklaard de dienst zo te hebben ingesteld dat Google het laatste octet van het IP-adres van de smart tv verwijdert voordat het IP-adres wordt opgeslagen.[156] "*Omdat TP Vision tevens de optie van 'gegevens delen' heeft uitstaan, worden de opgeslagen gegevens van televisies door Google uitsluitend gebruikt ten behoeve van de levering van Google Analytics rapporten aan TP Vision.*"[157]

TP Vision geeft het Device ID niet door aan Google.[158] TP Vision verklaart geen gebruik te maken van diensten van Google als Google AdWords en Google Adsense.[159] Volgens TP Vision is sprake van *first party* cookies, die niet gebruikt kunnen worden om gedrag over meerdere websites aan elkaar te koppelen.[160]

Blijkens het privacystatement van TP Vision gebruikt TP Vision de Analytics-dienst om interactie met het service portal en met een mobiel apparaat (via de My Remote TV afstandsbedieningsapp) in kaart te brengen.[161] Tijdens het onderzoek ter plaatse heeft TP Vision toegelicht de statistieken te gebruiken om inzicht te krijgen welke

[155] Naleving van het bepaalde in artikel 76 e.v. van de Wbp (doorgifte) valt buiten de scope van dit onderzoek door het CBP.
[156] Een 'octet' van een IP-adres is (in de huidige IPv4 architectuur) een 8-bits binair getal. Het bestaat uit maximaal drie cijfers (van 0 tot 255). Na het verwijderen van het laatste octet behoort het IP-adres dus tot een groep van maximaal 256 apparaten. Bij IPv6-adressen verwijdert Google de laatste 80 van de 128 bits. Bron: http://support.google.com/analytics/bin/answer.py?hl=en&answer=2763052
[157] Zienswijze TP Vision van 5 april 2013, p. 5.
[158] Idem, p. 8.
[159] Idem, p. 5.
[160] Idem, p. 8.
[161] Smart tv privacy statement, 12 oktober 2012 en ongewijzigd op 1 mei 2013 (Engelstalig), onder het kopje 'Data collected during use': "We use Google Analytics to store and monitor your interaction with the Portal by means of your Device or Mobile Device. This data is not linked to the Consumer-ID or the Device-ID (...)."

apps op welk tijdstip worden gebruikt, absolute en relatieve clicks op websites en unieke bezoekers van/bezoeken aan websites. Uit de zienswijze van TP Vision blijkt dat de Google Analytics aanvullend zijn op de door IBM gegenereerde statistieken, en dat deze vooral zien op de interactie met de apps in de *App Gallery*. "*Gezien het feit dat de Google Analytics code uitsluitend op de webpagina's van APP Gallery in de Services Portal is geïmplementeerd, is op basis van de verkregen informatie alleen duidelijk dat een televisie gebruiker heeft geklikt op een icoon van een APP.*"[162] Omdat TP Vision niet beschikt over de IP-adressen in de Google Analytics-rapporten, kan deze informatie niet worden verbonden aan een individuele televisie. "*Dit zou uitsluitend kunnen indien de eigen log gegevens van TP Vision voor de betreffende pagina van de APP Gallery worden verbonden met de Google Analytics rapporten, maar het Smart TV systeem is daarvoor niet ontworpen.*"[163]

TP Vision heeft verklaard de standaard terms en conditions van Google te hebben ondertekend voor het gebruik van Google Analytics en geen aparte bewerkersovereenkomst te hebben gesloten met Google.[164] Bij mail van 4 april 2013 heeft Google Nederland in reactie op een verzoek van TP Vision schriftelijk geweigerd om een bewerkersovereenkomst te sluiten, omdat het volgens Google geen persoonsgegevens betreft.[165]

Bij hardwareproblemen levert TP Vision zelf ondersteuning aan gebruikers. De gebruiker kan de servicedesk van TP Vision bellen en het MAC-adres van zijn toestel doorgeven voor remote support, of zijn naam en adresgegevens doorgeven om een monteur van TP Vision langs te laten komen.[166]

Installatie van de Philips smart tv

Tijdens het onderzoek ter plaatse en tijdens de twee controle-onderzoeken naderhand heeft het CBP de installatieprocedure doorlopen van een Philips smart tv met standaardinstellingen. Hieruit is het volgende gebleken, zoals fotografisch vastgelegd van het beeldscherm, nagekeken in de logfiles en verklaard door TP Vision.

Bij eerste installatie van het toestel (en elke keer daarna dat het toestel wordt aangezet) meldt het toestel zich bij het device portal. Hier krijgt het toestel (van Philips) een vaste Device ID en een Consumer ID. Vervolgens wordt via het device portal een vaste URL in de browser geladen (de server sign-on URL), zodat de gebruiker zijn beginscherm te zien krijgt. Dit beginscherm bevat het 'service portal' met betalingsmogelijkheden, advertenties en de recommenderdienst. Daarnaast krijgt de gebruiker via dit beginscherm toegang tot de tv-gids, een reeks apps[167] en de App Gallery met toegang tot de browser en alle beschikbare apps.

---

[162] Zienswijze TP Vision van 5 april 2013, p. 5.
[163] Idem, p. 5-6.
[164] Verklaring TP Vision tijdens het onderzoek ter plaatse, zoals bevestigd door het CBP bij brief van 16 oktober 2012.
[165] Brief TP Vision van 8 mei 2013, bijlage 3.
[166] Verklaring TP Vision tijdens het onderzoek ter plaatse.
[167] Tot de apps die meteen zichtbaar zijn in de App Gallery behoren naast de browser onder andere Twitter, Skype, Facebook, YouTube, Uitzending Gemist, een weer- en navigatieapp en een aantal specifieke binnen- en buitenlandse tv-zenders.

Bij het laden van het beginscherm wordt (via de server sign-on URL) naast de Device ID en de Consumer ID ook nog toestelspecifieke informatie geladen[168], de registratiestatus, of de gebruiker de algemene voorwaarden heeft geaccepteerd en het land dat de gebruiker heeft ingesteld.[169] Deze informatie wordt uitgelezen van het toestel.

Bij het laden van het beginscherm worden verschillende cookies opgeslagen in de browser op het toestel. Het betreft onder meer twee Google Analytics cookies en sessiecookies door het service portal en (bij gebruik ervan, zoals hieronder beschreven) door de tv-gids. Het service portal plaatst een tijdelijke, zogenoemde 'SESO'-sessiecookie. De inhoud van deze cookie is [VERTROUWELIJK].[170]

Tijdens de eerste aanmelding wordt de gebruiker onder meer gevraagd een land in te stellen, verbinding te maken met het Wifi-netwerk, de gebruiksvoorwaarden te accepteren en wordt de gebruiker gevraagd zich te registreren.

[168] PowerPointpresentatie TP Vision, p. 19. Het betreft de manufacturer ID en de profile ID (met de firmware ID, firmwareversie en typenummer van het toestel).
[169] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 22 en 24 en PowerPointpresentatie TP Vision tijdens het onderzoek ter plaatse, p. 19 en 20.
[170] TP Vision screenshots van systeemoverzicht cookies tijdens het onderzoek ter plaatse van 9 oktober 2012, met uitgelichte inhoud SESO-cookie, p. 3.

Het registratiescherm bevatte tot medio april 2013 de volgende hoofdtekst:

"Club Philips
Voordelen van registratie:

- *Automatische back-up van uw persoonlijke voorkeuren*
- *Gratis software updates*
- *Ontvangst van relevante productinformatie"*[171]

Op 3 juni 2013 heeft het CBP tijdens een tweede controle-onderzoek vastgesteld dat de tekst van het registratiescherm was gewijzigd (voor nieuwe en bestaande gebruikers):

"Club Philips
Voordelen van registratie:

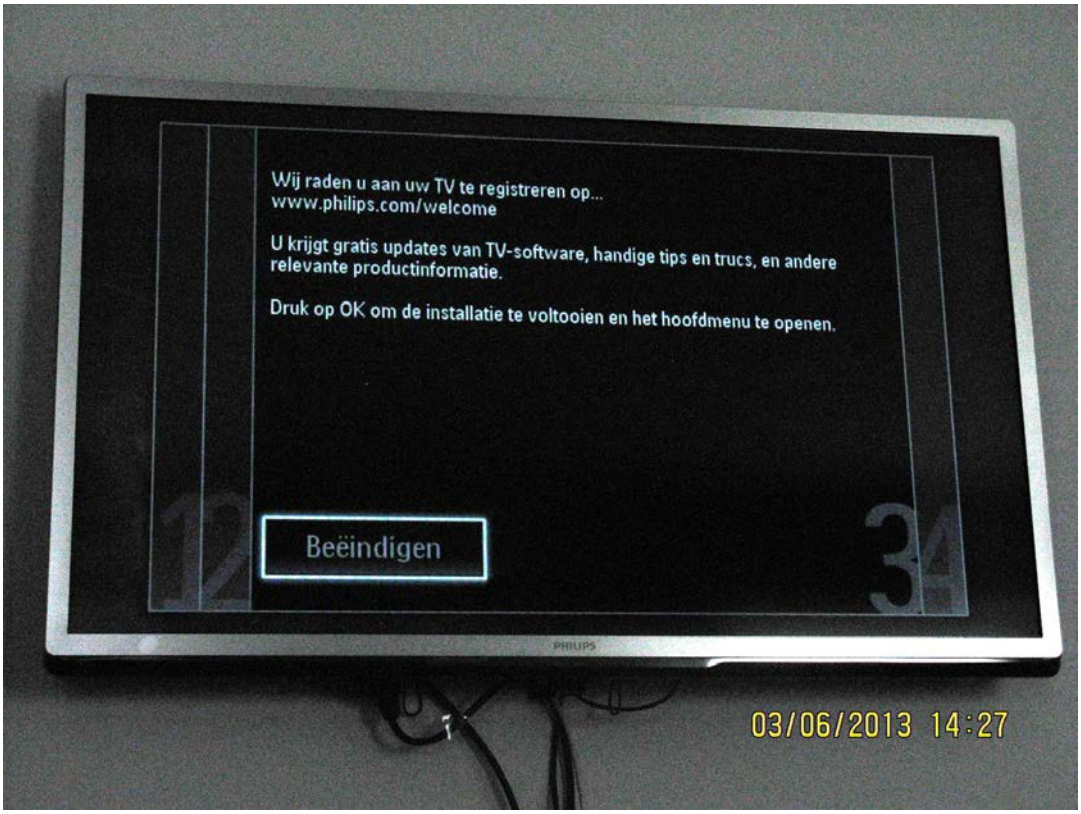
- *Automatische backup van uw persoonlijke voorkeuren*
- *Ontvangst van relevante productinformatie"*[172]

Registratie geschiedt door een e-mailadres in te vullen. Op dat e-mailadres ontvangt de gebruiker een hyperlink naar een Philips registratiewebsite.[173] Het scherm bevat daarnaast een hyperlink naar het privacybeleid van Philips, en opties om de registratie uit te stellen of te weigeren.[174]

Tijdens controle-onderzoek op 3 juni 2013 bleek dat gebruikers, als zij ervoor kiezen om registratie te weigeren of uit te stellen, voor het voltooien van de installatie (alsnog) het advies krijgen om zich bij Philips te registreren, "v*oor gratis updates van TV software, handige tips en trucs, en andere relevante productinformatie.*" (zie illustratie 1).[175]

[171] Onderzoek ter plaatse van 9 oktober 2012, foto 36 van het beeldscherm
[172] Controle-onderzoek van 3 juni 2013 door het CBP op een nieuwe Philips smart tv, aanschafdatum 2 februari 2013, type Philips 40PFL5507K, met firmware versie Q554E-0.97.0.0, met als releaseopmerking Release for TV550R4: Q554E-097.0.0_bld80a. De 'Generation date' was (opnieuw) niet ingevuld, foto 1 van het beeldscherm.
[173] Tijdens het onderzoek ter plaatse van 9 oktober 2012 heeft het CBP een e-mailadres ingevuld en de toegezonden website bezocht en vastgelegd (foto's 40 en 41 van het beeldscherm).
[174] Onderzoek ter plaatse van 9 oktober 2012, foto 42 van het beeldscherm.
[175] Controle-onderzoek van 3 juni 2013, foto 19 van het beeldscherm.

Illustratie 1: advies registratie bij Philips



Het Device ID is gebaseerd op het MAC-adres van het toestel (het interne door de fabrikant vastgelegde unieke hardwareadres).[176] Zowel het Device ID als het Consumer ID worden door Philips aangemaakt. Het Consumer ID kan door Philips gekoppeld worden aan NAW-gegevens, als een klant ervoor kiest om zich via de smart tv (bij Philips) te registreren.[177] TP Vision heeft verklaard en het CBP heeft vastgesteld dat die registratie niet noodzakelijk is. De internetfunctionaliteit kan ook worden gebruikt zonder registratie.[178]

Gebruik van de Philips smart tv

Bij het gebruik van de Philips smart tv worden de volgende gegevens verwerkt:

Als een gebruiker een nieuwe app toevoegt aan zijn beginscherm of op een app klikt, bezoekt hij feitelijk een webpagina. Uit de logfiles van het Service Portal blijkt dat TP Vision in dat geval het IP-adres van de internetverbinding van de gebruiker van de tv ontvangt, de hostname van de app of website en datum en tijdstip van het bezoek aan

[176] Het betreft de 64-bits Extended Unique Identifier (EUI-64). Een MAC-adres bestaat uit 48 bits. Om van het MAC-adres een EUI-64 te maken, wordt het MAC-adres in twee delen geknipt en een standaard 16-bits hexadecimale waarde toegevoegd, namelijk 0xFFFE.
[177] De verwerking door Philips van consumentengegevens is gemeld bij het CBP onder nummer m1166347, laatste melding 8 maart 2012, versienummer 3.0. Deze (zelfstandige) gegevensverwerkingen door Philips vallen buiten de scope van dit onderzoek.
[178] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 20. Tijdens het onderzoek ter plaatse heeft het CBP dit geverifieerd, evenals tijdens de controle-onderzoeken van 25 februari 2013 en 3 juni 2013.

de website/app.[179] TP Vision ontvangt ook de lijst met bookmarks die een gebruiker aanlegt.[180] Deze gegevens worden opgeslagen en in een database record gekoppeld aan het Device ID en het Consumer ID.[181]

Ten aanzien van het IP-adres verklaart TP Vision "*dat de Service Portal, zoals elke website ter wereld, het IP adres van de bezoeker ontvangt, echter de Service Portal slaat deze informatie niet op (zoals getoond tijdens uw bezoek in oktober 2012 en in de geleverde documentatie).*"[182]

Hiermee in tegenspraak is de verklaring in het nieuwe Privacy Statement van 1 mei 2013: "*As part of this traffic we receive the IP address of your Internet connection and the language and country that has been configured in your Device. This information is stored in a database on the Platform. We also store IP addresses within the database of the IP-EPG. server log* [onderstreping toegevoegd door het CBP]."[183]

De bewerkersovereenkomst van TP Vision met IBM (van mei 2013) vermeldt dat IBM de IP-adressen verwerkt en permanent bewaart.[184]

TP Vision verklaart dat zij ten aanzien van webverkeer uitsluitend de webadressen verwerkt die door de gebruiker van de tv handmatig worden ingegeven in de browser. *"Dit houdt bijvoorbeeld in dat als een consument http://www.ns.nl ingeeft, uitsluitend deze URL wordt opgeslagen maar niet bijvoorbeeld http://www.ns.nl/reizigers/ reisinformatie (als hij op bijvoorbeeld op zoek is naar reisinformatie)."*[185]

---

[179] Zienswijze TP Vision van 5 april 2013, p. 7. Vergelijk ook het TP Vision smart tv privacy statement van 12 oktober 2012 (en ongewijzigd gebleven in het nieuwe Privacy Statement van 1 mei 2013): "Each URL that is inserted by you in the navigation bar of the browser of your Device is stored on the Platform and linked to the Consumer-ID and the Device-ID. When you click on an APP we will only store this click and the date and time on which you performed the click. Your APP clicks are stored in a database record, linked to the Consumer-ID and the Device-ID."

[180] TP Vision screenshots van logfiles van het Service Portal tijdens het onderzoek ter plaatse, p. 4, rubrieken 'URL', 'URL_BOOKMARKS' en 'URL_HISTORY'.

[181] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 27 en 28.

[182] Zienswijze TP Vision van 5 april 2013, p. 7. Tijdens het onderzoek ter plaatse en in haar reactie van 9 oktober 2012 op het verzoek om inlichtingen van het CBP verklaarde TP Vision dat IBM geen IP-adressen opsloeg. "Deze [IP-adressen, toevoeging door het CBP] worden bijgehouden door Gracenote GmbH (…) in de server logs voor de recommendation engine (…) en door Akamai in zijn server logs. Inkomend Internet verkeer op Net TV Services Portal wordt via de systemen van Akamai afgeleverd bij IBM Nederland B.V. (…). Hoewel IBM gebruik maakt van een reverse proxy, en dus het IP verkeer in principe anoniem is, ontvangt IBM door middel van een speciale http header het IP nummer van de betreffende tv. IBM slaat dit IP nummer echter niet op. Het platform is ook niet zodanig ontworpen dat dit nummer kan worden opgeslagen. IBM noch TPVN hebben dan ook toegang tot dit IP nummer (…)."

[183] TP Vision Smart TV Privacy Statement 1 mei 2013, URL: http://www.tpvision.com/images/Legal_information/SMARTTVPrivacyStatementMay2013.pdf

[184] Data Processor Agreement IBM, ondertekend 6 mei 2013, Annex A. IP address (…) These values are stored permanently in the service Portal to ensure consistency of the user experience.

[185] Reactie TP Vision van 18 oktober 2012 op de schriftelijke weergave van zijn verklaringen door het CBP van 16 oktober 2012, p. 1.

De rest van het webverkeer tussen een gebruiker en een website of app loopt via het publieke internet, zonder dat TP Vision hier inzage in heeft.
TP Vision houdt verder de volgorde bij van apps op het beginscherm, en registreert wijzigingen die een gebruiker hierin aanbrengt.[186]

Bij het tv-kijken staat de door TP Vision ontwikkelde IP EPG (hierna: digitale tv-gids) centraal. Via deze gids plaatst TP Vision elke drie tot vijf minuten een cookie in de browser op de tv. Deze sessiecookies worden gelezen en opgeslagen in de door GraceNote bijgehouden logfiles van het kijkgedrag. Deze cookies bevatten onder andere een uniek sessionID, de laatste keer dat het toestel is aangezet in combinatie met het tijdstip, de zender (op basis van door Gracenote aangeleverde zender-ID's) en bekeken programma (op basis van de door Gracenote aangeleverde unieke nummers en titels van die uitzendingen).

Tegelijk met deze cookies wordt (door het Service Portal) telkens ook een SESO-cookie verstuurd, dat het Consumer-Device ID bevat.[187] In haar zienswijze licht TP Vision toe dat deze SESO-cookies (van het Service Portal) op een enkele uitzondering na, niet worden gedeeld met de server waarop de IP-EGP-cookies staan. "*Deze uitzondering betreft een cookie waarmee de IP-EPG aan de Service Portal doorgeeft dat de gebruiker de IP-EPG heeft geactiveerd.*"[188]

De logfiles van de cookies die worden geplaatst en uitgelezen door de tv-gids stellen TP Vision in staat om een overzicht te maken van het kijkgedrag per toestel, dat wil zeggen wanneer de televisie wordt aangezet, welke televisieprogramma's worden bekeken, hoe de gebruikers wisselen tussen tv-kanalen. Ook registreert TP Vision per Consumer-Device ID welke televisieprogramma's op welk tijdstip zijn opgenomen, voor welke programma's de kijker een reminder heeft ingesteld, op welke plaats een gebruiker een zender heeft geïnstalleerd in zijn zendermenu. Uit de logfiles van de digitale tv-gids blijkt tevens dat TP Vision van gebruikers van de tv-gids het IP-adres ontvangt en vastlegt van de internetverbinding van de gebruiker van de tv.[189]

---

[186] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 23 Dit blijkt ook uit de TP Vision screenshots van logfiles van het Service Portal, rubriek 'Favorite Services'. De verwerking is als volgt weergegeven in het smart tv privacy-statement van 12 oktober 2012 (ongewijzigd per 1 mei 2013). Onder het kopje 'APP placement' verklaart TP Vision: "As part of the regular functionality of the Portal you can manually arrange the order in which APPs are displayed on your home screen in the Portal. We will store your initial arrangement and any changes you make afterwards, linked to the Consumer-ID and the Device-ID." Zie de **Bijlage** bij dit rapport.

[187] TP Vision screenshots van de cookieopslag in de browser op de tv. Het betreft cookies van het domein epgacc.corio.com, met de namen 'SESO, ASP.NET_SessionID, termsofuse, httpUserToken, httpsUserToken en channellistfavid. Vanuit het domein corio.com worden daarnaast de cookies ipepgshared, privacystatus en weatherinfo geplaatst en gelezen. Daarnaast worden vanuit het domein epgacc.corio.com twee permanente cookies geplaatst ten behoeve van gebruik door Google Analytics.

[188] Zienswijze TP Vision van 5 april 2013, p. 7.

[189] TP Vision Smart tv privacy statement van 12 oktober 2012 (ongewijzigd in de nieuwe versie van 1 mei 2013): "We also store IP addresses within the database of the IP-EPG. server log" en idem in toelichting in de e-mail van TP Vision van 15 oktober 2012: "In het privacy

De cookies die het kijkgedrag vastleggen, worden uitgelezen door Gracenote ten behoeve van het tonen van aanbevelingen in de recommenderdienst.
Daarnaast ontvangt Gracenote via TP Vision informatie over het kijkgedrag via de aanbieders van *video on demand*-diensten (onlinevideotheken) en van de aanbieders van 'uitzending gemist'-apps.[190] Deze categorie apps is op het toestel toegankelijk via de knop 'Online TV'. Uit de logfiles blijkt dat TP Vision over deze apps de volgende gegevens verwerkt: het Device ID, het Consumer ID, datum-tijdstempel, de naam van de uitzending en het uitzendings-ID, dat wil zeggen het unieke nummer van elke uitzending zoals dat door Gracenote wordt aangeleverd met de televisiegegevens.[191]

TP Vision heeft verklaard alleen anonieme productprofielen bij te houden op basis van Consumer ID/Device ID en typenummer van het toestel. "*Het profiel op basis van dit type nummer wordt bijgehouden om alleen die content te tonen aan het device die beantwoordt aan de technische kenmerken van het device. Er worden geen profielen bijgehouden op naam van een individuele consument. Deze profielen worden uitsluitend aangevuld met informatie omtrent afgenomen video on demand programma's (...).*"[192]

In haar **zienswijze** op het rapport voorlopige bevindingen schrijft TP Vision dat het softwareplatform waar Smart TV op draait, per televisie wordt ingericht en niet per toeschouwer of gebruiker. "*Er zijn geen aparte inlog-codes of inlog-profielen per individuele gebruiker (zoals dat bijvoorbeeld bij een computer operating systeem als Microsoft Windows wel het geval is of kan zijn), waardoor niet zondermeer kan worden nagegaan welke persoon nu precies gebruik maakt van de televisie of de Smart TV functionaliteiten. De notie dat gegevens die door de individuele televisie met (de servers van) TP Vision (of haar leveranciers zoals IBM) worden gedeeld per definitie herleidbaar zijn tot een specifiek identificeerbare natuurlijke persoon is daarom niet altijd correct. TP Vision weet niet wie er voor de televisie zit en een televisie kan worden gebruikt door een huishouden met een vader, moeder en twee kinderen, maar kan ook in een studentenhuis met 14 bewoners staan. In een groot aantal gevallen (met meer dan 1 potentiële tv kijker) zullen de door TP Vision opgeslagen gegevens dan ook, al dan niet via bewerkelijke omwegen, hoogstens (in geaggregeerde vorm) per huishouden kunnen worden vastgesteld.*"[193]

Het CBP heeft vastgesteld dat het mogelijk is om cookies op het toestel te wissen. Hiervoor moet een gebruiker de volgende stappen doorlopen: [configuratie] [netwerk-instellingen] [wis internetgeheugen][wachtwoorden, cookies en geschiedenis wissen, ok / annuleer]. Aanvullend heeft TP Vision verklaard dat deze optie niet leidt tot het wissen van de browsergeschiedenis.[194] Indien een gebruiker dat wel wil, zijn er twee mogelijkheden om de browsergeschiedenis te verwijderen: ofwel handmatig de *icons*

---

statement is nu duidelijk gemaakt dat IP nummers van devices ook een informatie veld zijn in de IP-EPG database."

[190] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 32.
[191] TP Vision screenshots van IP-EPG-logfiles tijdens het onderzoek ter plaatse.
[192] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 42.
[193] Zienswijze TP Vision van 5 april 2013, p. 2.
[194] Reactie TP Vision van 18 oktober 2012 op de schriftelijke weergave van 16 oktober 2012 door het CBP van verklaringen tijdens het onderzoek ter plaatse, p. 2.

verwijderen van bezochte apps/websites of de tv opnieuw installeren vanaf fabrieksinstellingen.[195]

Tijdens het onderzoek ter plaatse heeft het CBP de Twitterapp aangeklikt. Hierna verscheen de mededeling dat eerst de tv-gids moest worden geactiveerd.[196] Bij dit activeren moet de gebruiker akkoord gaan met de algemene voorwaarden van Gracenote.

Desgevraagd heeft TP Vision getoond dat het mogelijk is om de recommenderdienst uit te zetten. De gebruiker kan, indien de cursor in het aanbevelingsmenu op het scherm staat, via de knop [Opties] op de afstandsbediening kiezen voor 'personalisatie uit'.[197]

Als een gebruiker de My Remote TV afstandsbedieningsapp gebruikt dan kan hij via zijn smartphone of tablet (hierna: apparaat) de tv-gids gebruiken en bijvoorbeeld zappen tussen zenders. Hierbij registreert TP Vision een (nieuw) uniek nummer, het Mobiel Device ID, dat gekoppeld wordt aan het Device ID.[198]

Op Apple-apparaten gebruikte TP Vision voorheen het ingebouwde UDID als uniek toestel herkenningsnummer (*Unique Device Identifier*), maar nu Apple het gebruik van dat nummer niet meer toestaat aan ontwikkelaars, gebruikt TP Vision het (door de app uitgelezen en gehashte) MAC-adres van het apparaat.[199] Op apparaten met het Android-besturingssysteem leest TP Vision het Android ID, een vast 64-bits nummer dat op het apparaat wordt gegenereerd en opgeslagen als het toestel voor het eerst wordt aangezet.[200]

Tevens registreert TP Vision de naam van het mobiele apparaat, zoals die door de eigenaar is ingevoerd. Uit de logfiles die het CBP tijdens het onderzoek heeft bekeken, bleek dat hierin namen voorkwamen, zoals 'iPad van [naam]'.[201]

Tijdens het onderzoek ter plaatse verklaarde TP Vision in de zeer nabije toekomst advertenties te gaan aanbieden via het service portal, via een eigen advertentieserver of via derde partijen (advertentienetwerken). TP Vision verklaarde dat zij daartoe session cookies wilde gebruiken met wisselend cookie-ID. De cookies zouden dan verdwijnen als het toestel werd uitgezet of in stand-by-stand ging. Naderhand verklaarde TP Vision dat de voorgenomen implementatie geen mogelijkheid bood tot

---

[195] Idem.
[196] Onderzoek ter plaatse van 9 oktober 2012, foto 51 van het beeldscherm.
[197] Idem, foto 75 van het beeldscherm.
[198] De app is niet door het CBP onderzocht en valt buiten de scope van dit onderzoek.
[199] Het MAC-adres van het mobiele apparaat wordt door de app gehasht. TP Vision kan uit deze hash niet het MAC-adres herleiden, maar gebruikt de hash als "a unique, invariable (lifetime fixed) identifier of each device." E-mail TP Vision van 29 oktober 2012.
[200] TP Vision verklaart dat sommige fabrikanten hetzelfde Android ID-nummer geven aan een reeks toestellen en dat het nummer daarom minder uniek is dan het voor Apple-toestellen gemaakte ID op basis van het MAC-adres. Idem.
[201] TP Vision screenshot van IBM logfile tijdens het onderzoek ter plaatse van 9 oktober 2012.

het gebruik van tijdelijke session cookies. "*Wij gaan nu de advertentie server implementeren op basis van een regulier cookie. TPVN zal dit cookie inregelen in overeenstemming met artikel 11.7a van de Telecommunicatiewet.*"[202] In de melding bij het CBP heeft TP Vision als categorie persoonsgegevens opgenomen "Advertentie kijk en klik gedrag per Device-ID."

Medio januari 2013 gaf TP Vision een nadere toelichting op de soorten advertentiegegevens die met de (permanente) cookies worden verwerkt.

"*TP Vision begint in maart 2013 met een advertentie pilot. (…) In de advertentie pilot wordt alleen gebruik gemaakt van profielen die zijn gebaseerd op het type tv toestel. (…) Aan derden (Advertisers en Publishers) worden de volgende geaggregeerde advertentiegegevens verstrekt. Deze gegevens zijn niet voorzien van een unieke identifier zoals bv een cookie id of een Device ID en zijn uitsluitend bedoeld om te kunnen afrekenen met de betreffende derde.*
Advertentiegegevens:

- *Impressies*
- *Viewage (kijktijd naar een advertentie)*
- *Engagement (interactie met een advertentie)*
- *CTR (Click Through Rate).*

TP Vision gaat dus geen zogenaamde tracking cookies plaatsen."[203]

In haar zienswijze benadrukt TP Vision dat de server die toeziet op het leveren van advertenties geen Device ID zal ontvangen.[204]

TP Vision heeft begin april 2013 verklaard: "*Momenteel worden op beperkte schaal cookies gebruikt bij het aanbieden van advertenties op de Smart TV Portal. Deze functionaliteit is pas onlangs aan het Smart TV Portal toegevoegd en bevindt zich nog in een testfase. De in dit kader gebruikte cookies dienen ter voorkoming van het herhalen van advertenties op hetzelfde scherm, of, indien meerdere advertenties tegelijkertijd getoond kunnen worden, het gelijktijdig plaatsen van meerdere dezelfde advertenties op hetzelfde scherm. (…) Van een koppeling van kijk en/of klikgedrag aan bepaalde advertenties, of het volgen van gebruikers over verschillende pagina's of applicaties, is geen sprake.*

TP Vision is voornemens het gebruik van advertenties in de nabije toekomst (binnen een paar maanden) uit te gaan breiden. Alvorens deze meer uitgebreide vorm van advertenties gebruikt gaat worden, zal TP Vision haar systeem zodanig inregelen dat het vragen om ondubbelzinnige toestemming voor dergelijke cookies wordt opgenomen in de registratie-flow, en dat bestaande gebruikers een pop-up te zien zullen krijgen waarin zij eveneens worden verzocht om al dan niet hun (ondubbelzinnige) toestemming te geven voor het gebruik van deze cookies."[205]

Tijdens het onderzoek ter plaatse verklaarde TP Vision ook op korte termijn betaalmogelijkheden te gaan aanbieden via een 'smart tv payment account'. Desgevraagd door het CBP, mede naar aanleiding van berichten in de media in

[202] E-mail TP Vision van 15 oktober 2012.
[203] Reactie TP Vision van 16 januari 2013 op verzoek om inlichtingen van het CBP, p. 2.
[204] Zienswijze TP Vision van 5 april 2013, p. 8.
[205] Idem, p. 15.

november 2012, verklaarde TP Vision dat de betaalmogelijkheden inderdaad in gebruik waren genomen. Om via de smart tv te kunnen betalen, dienen gebruikers hun naam, adres, land, mobiele telefoonnummer, e-mailadres en betaalgegevens zoals creditcardnummer te geven. Deze informatie wordt, samen met betalingsgegevens, gekoppeld aan het Device ID. Deze dienst is uitbesteed aan MPP Global.[206]

TP Vision heeft verklaard dat zij zich baseert op de grondslagen uit artikel 8, onder b (noodzakelijk voor de uitvoering van een overeenkomst), c (noodzakelijk voor de uitoefening van een wettelijke verplichting) en f (noodzakelijk voor de behartiging van haar gerechtvaardigd belang), van de Wbp voor de gegevensverwerkingen die ontstaan door en voortvloeien uit het gebruik van de Philips smart tv.[207]

2.2.3 Informatie

Het CBP heeft bij aanvang van het onderzoek vastgesteld dat TP Vision op zijn publiek toegankelijke websites (.com en .nl) geen informatie gaf over de gegevensverwerking via de Philips smart tv. De websites van TP Vision bevatten weliswaar een privacystatement, maar dat zag alleen op de gegevensverwerking ten aanzien van bezoekers van de website van TP Vision.[208] Ook de specifieke op consumenten gerichte website van Philips over deze smart tv's bevatte geen informatie over aard en omvang van de gegevensverwerking.[209] Het CBP heeft bij aanvang en gedurende het onderzoek met zoekmachines gezocht met de trefwoorden 'Philips smart tv' en 'TP Vision', al dan niet in combinatie met de trefwoorden 'privacy' en 'gegevensverwerking', maar geen verwijzingen gevonden naar het privacybeleid.[210]

Op 3 juni 2013 heeft het CBP het onderzoek naar de publieke toegankelijkheid van de informatie herhaald. Hieruit is gebleken dat zoeken naar de combinatie 'privacy (of: gegevensverwerking) Philips smart tv' geen relevante resultaten oplevert. De combinatie 'TP Vision privacy' levert verwijzingen op naar de beknopte algemene privacyverklaring van TP Vision, die (nog steeds) vooral betrekking heeft op bezoek aan de website van TP Vision. De op 12 oktober 2012 geïntroduceerde en per 1 mei 2013 vernieuwde Privacy Statement en Cookie Policy blijken niet te vinden via de website www.tpvision.nl. De teksten zijn alleen te vinden op de website www.tpvision.com, onder het kopje 'legal information' in de *footer* van de webpagina (en niet onder het kopje daarvoor, 'privacy statement'). De teksten zijn alleen in het Engels beschikbaar.[211]

---

[206] Reactie TP Vision van 9 oktober 2012 op het verzoek om inlichtingen van het CBP, par. 34.
[207] Idem, par. 40.
[208] Privacy statement TP Vision, ongedateerd, forensisch vastgelegd op 20 november 2012, URL: http://www.tpvision.nl/privacy-policy. URL laatst bezocht op 28 februari 2013.
[209] Philips smart tv, URL: http://www.philips.nl/c/televisie/19568/cat/nl/, forensisch vastgelegd op 20 november 2012. URL laatst bezocht op 28 februari 2013.
[210] Het CBP heeft de resultaten van deze zoekopdrachten met behulp van de zoekmachines Google en Bing forensisch vastgelegd op 20 november 2012.
[211] Het CBP heeft de zoekacties op de websites van TP Vision en de resultaten van deze zoekopdrachten met behulp van de zoekmachines Google en Bing forensisch vastgelegd op 3 juni 2013.

Het CBP heeft vastgesteld dat een koper van een Philips smart tv in de verpakking geen informatie vindt met betrekking tot de gegevensverwerking. De verpakking bevat de volgende papieren met informatie in negen talen: een algemeen welkomstboekje van Philips met een eenregelige toelichting op de belangrijkste gebruiksmogelijkheden[212], een veiligheidshandleiding van Philips, een garantiebewijs van Philips en een montagehandleiding van Philips voor bevestiging van de tv aan de muur.

Desgevraagd door het CBP gaf TP Vision aan dat zij consumenten informeerde over de gegevensverwerkingen via de "*Terms of Use, de Privacy Statement en de Cookie Policy. Deze documenten zijn via de NetTV Services Portal bekend gemaakt en online gepubliceerd op http://tou.nettvservices.com/pages/ToU_V3_NL.html.*" Gevraagd naar informatie voor consumenten over specifieke gegevensverwerkingen door derden, bijvoorbeeld via apps, antwoordde TP Vision te informeren "*via het Privacy Statement van TPVN en via de privacy statements van de betreffende content partners.*"[213]

De Net TV Gebruiksvoorwaarden, die de gebruiker op het scherm bij eerste installatie moet accepteren voordat hij de smart tv kan gebruiken, bestaan uit de volgende onderdelen:

"(A) Gebruiksvoorwaarden; (B) Privacybeleid; (C) Auteursrechtbeleid; (D) Over ons." Deze voorwaarden, inclusief het privacybeleid, zijn volgens de tekst op het scherm na te lezen op http://tou.nettvservices.com.[214]

Uit controle-onderzoek van het CBP op 3 juni 2013 is gebleken dat de genoemde tou.nettvservices.com-website niet meer op deze wijze in gebruik is. De homepage toont een (technische) lijst van instellingen van de gebruikte webserver.[215]

TP Vision heeft verklaard dat deze webserver sinds de derde week van oktober 2012 (op een subpagina) een Nederlandstalige vertaling bevat van de Terms of Use.[216]

Punt (B) Privacybeleid bevat sinds die tijd[217] (sinds de derde week van oktober 2012) de volgende informatie:

---

[212] Het betreft de kopjes 'Sluit uw tv aan', 'Smart TV Apps', 'Video on demand', 'Uitzending gemist', 'Social Network', 'Skype', 'SimplyShare', 'Help' en 'Registreer'.
[213] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 46 en 48.
[214] Onderzoek ter plaatse van 9 oktober 2012, foto's 32-35 van het beeldscherm. Deze teksten zijn ongewijzigd gebleven, zoals vastgelegd door het CBP tijdens controle-onderzoeken op 25 februari en 3 juni 2013.
[215] Homepage bekeken op 3 en 5 juni 2013 en forensisch vastgelegd door het CBP op 5 juni 2013.
[216] Deze Nederlandstalige Gebruiksvoorwaarden zijn forensisch vastgelegd door het CBP op 1 november 2012, URL: http://tou.nettvservices.com/pages/ToU_v3_NL.html. Het CBP heeft de complete URL laatst bezocht op 5 juni 2013. Deze bevatte nog steeds de tekst gedateerd 12 oktober 2012.

Net TV hecht sterk aan de bescherming van de persoonlijk identificeerbare informatie die u aan Net TV verstrekt. Net TV vindt het ook belangrijk om u te informeren over hoe uw persoonlijke gegevens zullen worden gebruikt.

1. Vastlegging van kijkgedrag
Net TV heeft een functie die systematisch informatie vastlegt over programma's die op uw toestel worden bekeken. Deze informatie wordt gebruikt voor aanbevelingen van nieuwe programma's die op uw toestel te zien zijn, zoals:

Bekeken uitgezonden programma's
Gehuurde VoD-titels.
Bekeken online tv-programma's.

Als u er geen prijs op stelt dat het kijkgedrag op uw toestel wordt vastgelegd, kunt u deze functie in uw Net TV-portal deactiveren door de personalisatie-optie uit te schakelen. Als u deze niet uitschakelt, geeft u Net TV toestemming om het kijkgedrag op uw toestel te gebruiken om bovengenoemde aanbevelingen te doen.

2. Cookies
Ter verbetering van het Portaal kan Net TV gebruik maken van "cookies" voor het verzamelen en opslaan van een deel van uw persoonlijke gegevens. Ook maakt Net TV gebruik van zogenaamde Ad-Serving technologiebedrijven voor marketing- en reclamedoeleinden, zoals AdLINK. Deze Ad-Serving technologiebedrijven zullen ook gebruik maken van "cookies".

Een "cookie" is een klein tekstbestand dat naar uw Apparaat wordt verzonden en dat Net TV en de Ad-Serving technologiebedrijven in staat stelt om uw Apparaat bij uw volgende bezoek te herkennen, zonder dat u wordt lastig gevallen met een nieuw registratieverzoek. Indien u gebruik maakt van het Portaal, de Diensten en/of het open internet, verzamelt de cookie bepaalde "bezoekersinformatie" over u en slaat deze op, waaronder, echter zonder hiertoe beperkt te zijn, het Internet Protocol (IP) adres van het Apparaat, datum en tijdstip van uw gebruik van het Portaal, naam van de serviceprovider waartoe u via het Portaal toegang hebt verkregen en internetadres van de websites waartoe u via het open internet toegang hebt gekregen, doorgelinkt via het Portaal. De verzamelde en opgeslagen informatie wordt na enige tijd door Net TV en/of de Ad-Serving technologiebedrijven verwijderd.

Voor meer informatie over cookies, de bescherming van uw persoonlijke gegevens en keuzes over hoe deze gegevens zullen worden gebruikt, kunt u terecht op www.cookiecentral.com. gebruik daarvan het helpbestand van uw browser. Net TV adviseert u om het Privacybeleid te lezen voor meer informatie over het gebruik van uw persoonlijke gegevens verzameld door cookies die naar uw Apparaat worden verzonden; dit beleid is toegankelijk via: http://tou.nettvservices.com/privacy[218]

[217] Uit het eerste en tweede controle-onderzoek van het CBP, op respectievelijk 25 februari 2013 en 3 juni 2013, is gebleken dat de tekst op het scherm sindsdien ongewijzigd is gebleven.
[218] Net_TV Terms of Use, Engelstalig, print-out verstrekt door TP Vision gedateerd 8 oktober 2012, als bijlage 6 bij de reactie van TP Vision van 9 oktober 2012 op verzoek om

Tijdens het onderzoek ter plaatse van 9 oktober 2012 heeft het CBP doorgeklikt op bovengenoemde hyperlink naar de specifieke privacyverklaring. Deze pagina, 'Smart TV Privacy Statement', bevatte een Engelstalige verklaring, gedateerd 3 oktober 2012. TP Vision heeft in haar schriftelijke reactie op het inlichtingenverzoek verklaard dat dit Privacy Statement (en bijbehorende 'Smart TV Cookie Policy') recent waren opgesteld en voltooid. TP Vision heeft deze Engelstalige tekst nog aangepast op 12 oktober 2012.[219] Een print van deze tekst is opgenomen als **Bijlage I**.

Inhoud Privacy Statement oktober 2012

Het Smart TV Privacy Statement van oktober 2012 beschrijft onder het kopje 'identification numbers' als gegevens die TP Vision verwerkt het Consumer ID, het Device ID en het Mobile Device ID. In haar melding bij het CBP noemt TP Vision alle drie deze gegevens als persoonsgegevens (zie p. 26 van dit rapport). Ten aanzien van het Consumer ID stelt TP Vision dat dit voor haar geen persoonsgegeven is.[220] Ook ten aanzien van het Device ID schrijft TP Vision dat dit *"evenmin op zichzelf staand een persoonsgegeven is."*[221]

Het Privacy Statement beschrijft voorts de gegevensverwerking bij eerste aanmelding en bij het gebruik van de Philips smart tv, beschrijft de doeleinden van de verwerking (gelijk aan de hierboven beschreven inhoud van de melding bij het CBP), geeft aan dat via Akamai gegevens vanuit landen buiten de EU lokaal toegankelijk gemaakt kunnen worden waarbij de Akamaiservers zich ook buiten de EU kunnen bevinden en beschrijft de getroffen beveiligingsmaatregelen (SSL-versleuteling van het verkeer tussen de smart tv's en het device portal en naleving van de PCI-DSS Tier 1 standaard voor het verwerken van creditcardgegevens).[222]

Het Privacy Statement legt uit dat er cookies geplaatst kunnen worden op het toestel voor advertentiedoeleinden, door een eigen advertentieserver van TP Vision of door advertentieservers van derde partijen. Volgens het statement plaatst TP Vision geen advertentiecookies op het toestel zonder toestemming.[223]

TP Vision geeft verder aan IP-adressen te verzamelen en te bewaren in de online tv-gids, de URL's die gebruikers invoeren in de browser, en gebruik van apps. Onder het kopje 'Zap Behavior' legt TP Vison uit dat het op dat moment bekeken kanaal

---

inlichtingen van het CBP. TP Vision heeft daarbij de URL http://tou.nettvservices.com/pages/ToU_v3_NL.html gebruikt.

[219] TP Vision 'Smart TV privacy statement' gedateerd 12 oktober 2012, URL: http://tou.nettvservices.com/privacy/, URL laatst bezocht en vastgelegd op 4 maart 2013.

[220] Idem: "We receive the Consumer-ID without the corresponding registration data. As a consequence the Consumer-ID does not constitute personal data for us."

[221] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 7.

[222] De PCI-DSS Tier 1 standaard, de Payment Card Industry Data Security Standard is een beveiligingsstandaard die van toepassing is op de verwerking van creditcardbetalingen. Zie verder: https://www.pcisecuritystandards.org/. Naleving van de bepalingen in de Wbp ten aanzien van beveiliging (artikel 13) valt buiten de scope van dit onderzoek.

[223] TP Vision 'Smart TV privacy statement' gedateerd 12 oktober 2012, **Bijlage** bij dit rapport, meest recent forensisch vastgelegd op 4 maart 2013: "We will not set a cookie on your Device without your permission."

periodiek wordt vastgelegd in een cookie en dat deze gegevens opgeslagen worden in de recommenderdienst.[224]

TP Vision beschrijft in zijn Privacy Statement dat het bedrijf informatie krijgt over gehuurde films en bekeken 'gemiste' uitzendingen, gekoppeld aan het Device ID. Het statement bevat een toelichting op de mogelijkheid om gegevens over het kijk- en internetgedrag los te koppelen van de Consumer ID en de Device ID. Het statement beschrijft dat de gebruiker het toestel dan moet herinstalleren vanaf fabrieksinstellingen en zich in dat geval niet, of onder een andere naam, bij Philips moet registreren.

Het Privacy Statement bevat tevens een hyperlink naar een aparte Engelstalige cookie policy, eveneens gedateerd 12 oktober 2012.[225]

De cookiepolicy beschrijft alleen het gebruik van cookies die volgens TP Vision niet-functioneel zijn, waarbij functionele cookies als volgt worden gedefinieerd: "*Functional cookies are cookies that are needed specifically for the purpose of enabling a device to access and make use of the portal and content partner websites and for webservers to provide the right content to a device. Non-functional cookies are all other cookies.*" Volgens de policy gebruikt TP Vision de volgende cookies: Google Analytics, Zap Behavior en Advertising. Bij Zap Behavior geeft TP Vision de volgende toelichting: "*By opting-in for personalized recommendations, you give us permission for setting the cookie.*"

Wijzigingen Privacy Statement 1 mei 2013

Per 1 mei 2013 heeft TP Vision het Privacy Statement en de Cookie Policy uitgebreid, onder andere met informatie over de bewaartermijn van gegevens over het kijkgedrag en informatie over de betalingsgegevens.

TP Vision heeft de zinsnede verwijderd dat het Consumer ID geen persoonsgegeven is.

TP Vision noemt een bewaartermijn van drie maanden voor gegevens over het kijkgedrag, bezoek aan websites en gebruik van apps, gehuurde video's/films en catch-up TV (uitzending gemist). De bewaartermijn van drie maanden geldt ook voor IP-adressen, zowel ten aanzien van de IP-adressen die via het Portal worden verzameld, als voor de IP-adressen die via de recommenderdienst worden verzameld.[226]

---

[224] Idem: "Generally we store the currently watched channel periodically in a cookie on your Device. When this cookie is refreshed we receive a copy of the data stored in this cookie. This data is then stored within the recommendation engine of the Portal."

[225] Het CBP heeft deze URL forensisch vastgelegd op 12 november 2012.

[226] TP Vision Smart TV Privacy Statement van 1 mei 2013. "As part of this traffic we receive the IP address of your Internet connection and the language and country that has been configured in your Device. This information is stored in a database on the Platform. We also store IP addresses within the database of the IP-EPG. server log. This information is stored for a period not exceeding three (3) months, after which the data is either deleted or anonymized."

De bewaartermijn van door de gebruiker ingevoerde URL's en kliks op apps is permanent, tot de gebruiker zelf actie onderneemt. "*This information is stored until you remove the bookmarked pages from the overview using the options menu accessible with your remote control.*"

Specifiek over de recommenderdienst schrijft TP Vision dat informatie over het kijk- en zapgedrag periodiek met cookies wordt vastgelegd en dat het overzicht van het kijkgedrag drie maanden lang wordt bewaard gebruikt om aanbevelingen te doen, "*after which the data is either deleted or anonymized.*"

Aan de informatie over het gebruik van Google Analytics is toegevoegd dat Google de gegevens niet mag delen met derde partijen.

TP Vision heeft aan het nieuwe Privacy Statement het verwerken van betalingsgegevens toegevoegd aan de doeleinden van de verwerkingen. Over de bewaartermijn schrijft TP Vision "*stored in accordance with the retention requirements dictated by law for financial transactions.*"

TP Vision heeft tevens informatie toegevoegd dat gegevens doorgegeven kunnen worden naar de Verenigde Staten. "*To the extend such personal data is transmitted to the United States of America, we shall ensure that applicable outsourcing party either operates within the Safe harbor Rules, or is bound by adequate contractual documentation in line with mandatory EU model agreements. Furthermore, we do utilize the AKAMAI content distribution system to ensure that content relating to the Portal is cached nearby the geographic location of your Device, to improve speed and user experience. AKAMAI servers are also outside of the European Union.*"

TP Vision heeft ook aan de Cookie Policy informatie over de bewaartermijn toegevoegd: "*This data is then stored within the recommendation engine of the Portal for a period not exceeding three (3) months in order to make the personalized recommendations, after which the data is either deleted or anonymized.*"

2.2.4 Toestemming voor verwerken kijkgedrag

In reactie op het inlichtingenverzoek van het CBP heeft TP Vision verklaard: "*Vanaf 1 januari 2013, en zo mogelijk eerder, is een opt-in beleid van toepassing voor het opslaan van kijkgedrag. Indien een consument "gepersonaliseerde aanbevelingen" heeft aangezet binnen de NetTV Services Portal, zal TPVN regelmatig het kijkgedrag opslaan. (...) Het kijkgedrag wordt periodiek opgeslagen in een cookie op het device. (...) Voor bestaande devices die al gebruik maken van de Smart TV Portal zal afzonderlijk via een service boodschap om toestemming worden gevraagd.*"[227] TP Vision heeft tevens verklaard dat deze toestemming ook zal worden gevraagd voor het bijhouden van informatie van contentpartners over *video on demand* en 'uitzending gemist'-apps.

Het CBP heeft tijdens controle-onderzoek op 25 februari 2013 vastgesteld en vastgelegd dat deze toestemmingsvraag (nog) niet was ingevoerd. Er bleek geen

[227] Reactie TP Vision van 9 oktober 2012 op verzoek om inlichtingen van het CBP, par. 31 en 33.

nieuwe firmware beschikbaar om een eventuele nieuwe interface te kunnen onderzoeken.[228]

De eerste keer dat een gebruiker de tv-gids aanzette (en daarmee de recommenderdienst), verscheen een pop-up op het beeldscherm met de volgende inhoud:

> *Welkom bij het nieuwe Smart TV-bedieningspaneel. Het nieuwe bedieningspaneel bevat veel nieuwe functies, waaronder de Kijktip service. Hiermee wordt u geattendeerd op de beste nieuwe films en tv-programma's, waarbij wordt uitgegaan van uw eerdere kijkvoorkeuren op dit toestel. Als u deze persoonlijke kijktips wilt uitschakelen, kunt u dat doen in het menu Opties."*[229]

Deze pop-up verdween na 10 seconden.

Vervolgens diende een gebruiker akkoord te gaan met de algemene voorwaarden van de tv-gids. Deze algemene voorwaarden beschreven onder het kopje "2. De werking van de service" dat Gracenote zich inspant om de juiste data te leveren maar niet aansprakelijk is voor het niet-functioneren, en dat Gracenote evenmin verantwoordelijk is voor de juiste set-up of verbinding. Deze voorwaarden bevatten geen beschrijving van de gegevensverwerking, waaronder het plaatsen en uitlezen van informatie van de eindapparatuur van de gebruiker.[230]

Het CBP heeft tijdens het onderzoek ter plaatse, en nogmaals tijdens het eerste controle-onderzoek naar een Philips smart tv op 25 februari 2013, vastgesteld dat TP Vision geen andere informatie of pop-ups aanbood waarmee de gebruiker werd geïnformeerd over het feit dat er (door verschillende partijen) automatisch gegevens worden geplaatst en uitgelezen op de Philips smart tv. Noch bij eerste installatie, noch tijdens gebruik van het toestel kreeg de gebruiker keuzevragen voorgelegd met betrekking tot het plaatsen op en uitlezen van informatie van het toestel.

Het CBP heeft op 2 juni 2013 vastgesteld en vastgelegd dat TP Vision alsnog een toestemmingsvraag heeft ingevoerd, voor zowel nieuwe als bestaande gebruikers.[231] De letterlijke tekst luidt als volgt:[232]

---

[228] Eerste controle-onderzoek CBP op 25 februari 2013 op een nieuwe Philips smart tv, aanschafdatum 2 februari 2013, type Philips 40PFL5507K, met firmware versie Q554E-0.96.0.0, met als releaseopmerking Release for TV550R4: Q554E-0.96.0.0_BLD2c. De 'Generation date' was niet ingevuld.

[229] Onderzoek ter plaatse van 9 oktober 2012, foto 77 van het beeldscherm, opnieuw vastgelegd tijdens controle-onderzoek op 25 februari 2013.

[230] Onderzoek ter plaatse van 9 oktober 2012, foto 54 van het beeldscherm, Terms of Use Gracenote, opnieuw vastgelegd tijdens controle-onderzoek op 25 februari 2013.

[231] De gebruiker van het door het CBP onderzochte toestel heeft de pop-up met de toestemmingsvraag voor het eerst op 2 juni 2013 gezien. Tijdens het controle-onderzoek van 3 juni 2013 heeft het CBP het toestel gereset, en daarmee de situatie van een nieuwe gebruiker onderzocht en vastgelegd.

[232] Controle-onderzoek van 3 juni 2013, foto 23 van het beeldscherm.

Inschakelen persoonlijke aanbevelingen?

Uw Smart TV kan "persoonlijke aanbevelingen" leveren. Dit is een dienst die persoonlijke aanbevelingen doet aan de hand van uw kijkgedrag. Als u deze dienst activeert, dan houdt uw televisie uw kijkgedrag bij en slaat dit in een klein tekstbestand (cookie) op uw Smart TV. De inhoud van dit cookie wordt regelmatig aan onze servers doorgestuurd zodat de persoonlijke aanbevelingen kunnen worden opgesteld.

Als u op [inschakelen] klikt, dan zal de dienst voor persoonlijke aanbevelingen worden geactiveerd, en geeft u ons toestemming voor het gebruik van deze cookies. Als [uitschakelen] klikt, dan zal de dienst voor persoonlijke aanbevelingen niet worden geactiveerd, en zullen deze cookies niet worden gebruikt. U kunt deze instelling op een later tijdstip altijd wijzigen in het optie-menu van uw Smart TV.

Meer informatie over het gebruik van cookies voor de persoonlijke aanbevelingen vindt u in de Smart TV Privacy Statement en de Smart TV Cookie Policy die u op de Philips TV website kunt vinden.

[uitschakelen] [inschakelen]

3. BEOORDELING

In het hiernavolgende hoofdstuk van dit rapport worden de feitelijke bevindingen over de werkwijze van TP Vision, zoals beschreven in paragraaf 2.2, gekwalificeerd aan de hand van het in paragraaf 2.1 geschetste wettelijk kader.

Dit hoofdstuk begint met een beoordeling van de rol en verantwoordelijkheden van TP Vision. Dit wordt gevolgd in paragraaf 3.2 door een analyse van de gegevens die TP Vision verwerkt die persoonsgegevens zijn waarop de Wbp van toepassing is en, in paragraaf 3.3, welke handelingen met persoonsgegevens verwerkingen zijn. In paragraaf 3.4 komt aan de orde of de contractuele overeenkomsten die TP Vision met verschillende partijen heeft gesloten voor de verwerking van persoonsgegevens, voldoen aan de vereisten uit de artikelen 12 en 14 van de Wbp voor bewerkersovereenkomsten. In paragraaf 3.5 wordt beoordeeld of TP Vision voldoet aan haar informatieplichten jegens betrokkenen, conform het bepaalde in de artikelen 33 en 34 van de Wbp. Ten slotte wordt beoordeeld of TP Vision een grondslag heeft voor de verschillende gegevensverwerkingen als bedoeld in artikel 8 van de Wbp, in het bijzonder of TP Vision voldoet aan de vereisten voor rechtsgeldige toestemming voor het verzamelen, vastleggen en analyseren van kijk- en surfgedrag. Hierbij speelt ook het bepaalde in (artikel 11.7a van) de Tw een rol, omdat TP Vision deze gegevens deels verzamelt met behulp van verschillende cookies.

3.1 Verantwoordelijke

TP Vision bepaalt sinds 1 april 2012 doel en middelen voor het verzamelen en verwerken van gegevens over Nederlandse gebruikers van de smart tv.[233] TP Vision is daarmee de verantwoordelijke voor de gegevensverwerkingen via de Philips smart tv.[234]

Hoewel TP Vision in haar melding bij het CBP aangeeft dat Philips een bewerker zou zijn, vindt deze stelling geen ondersteuning in de feiten. Uit de overeenkomsten met TP Vision blijkt dat Philips de registratiegegevens gebruikt voor een eigen informatiesysteem (Club Philips), dat zich onttrekt aan de onderliggende contractuele relatie. Philips gebruikt de registratiegegevens voor eigen doelen zoals het nakomen van garantieverplichtingen en consumentenloyaliteitsprogramma's en kan daarom niet als bewerker van TP Vision worden beschouwd.[235]

Evenmin kan TP Vision als een bewerker van Philips worden beschouwd. Philips levert aan TP Vision een Consumer ID en een Device ID. TP Vision bepaalt zelfstandig de doeleinden waarvoor zij deze gegevens gebruikt, bepaalt de bewaartermijnen en kiest zelfstandig de derden aan wie zij deze gegevens verstrekt. Uit de toelichting op het wettelijk kader blijkt dat als een partij zeggenschap heeft over deze aspecten, zij als verantwoordelijke dient te worden aangemerkt.

Er is in de verhouding tussen Philips en TP Vision sprake van een integratie van verschillende verwerkingen, waarbij Philips en TP Vision een afzonderlijke verantwoordelijkheid dragen per (deel-)verwerking. Daarbij draagt TP Vision de verantwoordelijkheid voor het aanbieden van de (exclusieve) registratiemogelijkheid bij Philips en het verzamelen van de klantgegevens, omdat TP Vision daarbij zeggenschap heeft over de middelen van de registratie en de kwaliteit van de geboden informatie.

Dat sprake is van afzonderlijke en deels gezamenlijke verantwoordelijkheid (en niet van een bewerkersrelatie) blijkt tevens uit de marketingclausule tussen Philips en TP Vision. Daaruit blijkt dat TP Vision Philips de opdracht kan geven de klanten bijvoorbeeld per e-mail te benaderen (hostmailing), bijvoorbeeld om een software-update aan te kondigen, maar ook voor algemene marketingdoeleinden. Tevens kan TP Vision van Philips op verzoek inzage krijgen in de registratiegegevens voor intern marktonderzoek, "*e.g. to make consumer profiles*".[236] In dat geval dient TP Vision een bewerkersovereenkomst te tekenen met Philips. Hiervan is in het onderzoek niet gebleken. TP Vision heeft in haar zienswijze aangegeven dat te zullen doen als zij gebruik gaat maken van deze mogelijkheid.

---

[233] Op 1 april 2012 zijn de tv activiteiten van Philips, middels een Transitional Services Agreement, ondergebracht bij de joint venture TP Vision Holding B.V.
[234] In de melding bij het CBP van 16 oktober 2012 is TP Vision Netherlands B.V. ook als verantwoordelijke aangewezen.
[235] De verwerking door Philips van consumentengegevens is gemeld bij het CBP onder nummer m1166347, laatste melding 8 maart 2012, versienummer 3.0. Deze (zelfstandige) gegevensverwerkingen door Philips vallen buiten de scope van dit onderzoek.
[236] Zie p. 29 van dit rapport.

3.2 Persoonsgegevens

Het CBP heeft in paragraaf 2.2.2 van dit rapport (p. 27 e.v.) vastgesteld dat TP Vision in verschillende systemen en logfiles ten minste de volgende (combinaties van) gegevens met betrekking tot het gebruik van de Philips smart tv verwerkt:

Consumer ID (met bijbehorende registratiegegevens bij Philips)
Device ID
Mobile Device ID en naam van het mobiele apparaat
IP-adres van de internetverbinding van de smart tv
Registratiegegevens, betalings- en transactiegegevens (MPP Global)
Naam, adres, woonplaats (bij ondersteuning door de TP Vision service-desk)

Cookies met het Device ID en Consumer ID in combinatie met cookies die elke 3 tot 5 minuten het onlinekijkgedrag registreren via de elektronische programmagids, dat wil zeggen: a. nummer en titel van bekeken uitzendingen met zender b. reminders die ingesteld zijn voor favoriete uitzendingen c. opgenomen uitzendingen d. plaatsbepaling van zenders op het toestel. e. 'zap'-gedrag tussen zenders f. overzicht op welke tijdstippen/data de televisie wordt gebruikt.

Logfiles met tenminste het Device ID (vaak ook het Consumer ID) in combinatie met: a. gekozen apps, frequentie van gebruik van die apps en volgorde in het app-scherm b. in de browser ingevoerde URL's van websites

Databases met gegevens die van derde partijen worden verkregen met het Device ID in combinatie met: a. bekeken uitzendingen via 'uitzending gemist'-apps b. bekeken video's via *video on demand*-services

Getoonde aanbevelingen voor uitzendingen (recommenderdiensten via Gracenote)

Webstatistieken over bezoek aan websites en gebruik van apps, inclusief gebruik van de meegeleverde afstandsbedieningsapp (via het door IBM beheerde Service Portal en via Google Analytics)

Sinds de aanvang van de advertentiepilot in maart 2013:

Logfiles op basis van cookies van getoonde advertenties, kijktijd, interactie en eventuele kliks op advertenties

Het CBP heeft in paragraaf 2.2.2 van dit rapport (p. 27 e.v.) vastgesteld dat TP Vision de hierboven genoemde gegevens samenhangend met en voortvloeiend uit het gebruik van de Philips smart tv genereert/verzamelt, gebruikt, vastlegt en bewaart op

individueel persoonsniveau. Dit doet zij om individueel gebruik van de Philips smart tv in kaart te brengen.
Het Device ID, Consumer ID en Mobile Device ID met de naam van het mobiele apparaat (unieke klant- of toestel-identifiers), in onderlinge combinatie of in samenhang met gegevens over het onlinekijk- en internetgedrag (bekeken uitzendingen, gehuurde films, bezoek aan en gebruik door een betrokkene van apps en websites, tijdstippen van aan- en uitzetten van het toestel) zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon. De persoonsgegevens over het onlinekijkgedrag van betrokkenen zijn bovendien gegevens van gevoelige aard, omdat zij veel over personen zeggen.[237]

> In haar **zienswijze** bestrijdt TP Vision de kwalificatie van 'gevoelige gegevens', ondanks het feit dat het CBP en WP29 die term eerder hebben gebruikt, zoals toegelicht in voetnoot 237 onderaan deze pagina (voetnoot 170 van het Rapport voorlopige bevindingen). Volgens TP Vision zijn er juridisch alleen 'normale' en 'bijzondere' persoonsgegevens.[238]
>
> Met de term 'gevoelige gegevens' duidt het CBP gegevens aan die weliswaar niet zijn gedefinieerd als 'bijzondere persoonsgegevens' in artikel 16 van de Wbp, maar waarvan de verwerking grote impact op betrokkenen kan hebben. Deze term is in de parlementaire geschiedenis van de Wbp geïntroduceerd bij de bespreking van artikel 9 van de Wbp. "*Artikel 16 betreft de gegevens die uit hun aard gevoelig zijn. Daarnaast kunnen gegevens gevoelig zijn door de context waarin zij worden gebruikt, bij voorbeeld de gegevens omtrent iemands kredietwaardigheid of welstand. Hoe gevoeliger het gegeven, hoe minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijk doel.* "[239] De gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek kunnen een indringend beeld kunnen geven van iemands communicatiegedrag en soms ook iets zeggen over de inhoud van de communicatie. De gegevens raken ook aan de telecommunicatievrijheid.[240]

Op grond van de gegevens over bekeken uitzendingen, gebruikte apps en bezochte websites kunnen gedetailleerde profielen worden opgebouwd van iemands interesses,

---

[237] Vgl. Artikel 29-werkgroep WP 185, Opinion 13/2011 on Geolocation services on smart mobile devices van 16 mei 2011. URL: http://www.cbpweb.nl/downloads_int/wp185_en.pdf. Zie ook Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010 (z2010-00582), p. 34 e.v. URL: http://www.cbpweb.nl/downloads_rapporten/rap_2011_google.pdf. Zie ook Definitieve bevindingen Onderzoek door het CBP naar de verwerking van persoonsgegevens door Advance Concepts B.V. van 15 december 2009, p. 27 en 28, URL: http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf.
[238] Zienswijze TP Vision van 5 april 2013, p. 10.
[239] Kamerstukken II 1997/98, 25 892, nr. 3, p. 90.
[240] Memorie van Toelichting bij het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet, p. 17. URL: http://internetconsultatie.nl/briefentelecommunicatiegeheim.

sociale achtergrond, inkomen of gezinssamenstelling, inclusief voorspellingen die worden afgeleid uit het gedrag van andere, vergelijkbare mensen.

TP Vision kan deze gegevens aanwenden om de betrokkene op een bepaalde wijze te behandelen of het gedrag van die persoon te beïnvloeden, op een wijze die gevolgen heeft voor de rechten/belangen van de betrokkene.

Daarbij valt bijvoorbeeld te denken aan het gebruik van deze gegevens voor het tonen van gerichte aanbevelingen via de recommenderdienst. De gegevens worden dus door TP Vision gebruikt op een wijze die in het maatschappelijk verkeer de betrokkene raakt.

Verder kunnen de opgegeven voorkeuren van een betrokkene een indicatie zijn voor bijvoorbeeld zijn interesses, sociale achtergrond, inkomen of gezinssamenstelling. Dergelijke informatie kan worden gebruikt voor (direct) marketing- en profileringsdoeleinden. TP Vision kan bijvoorbeeld uit de bekeken uitzendingen afleiden of er jonge kinderen in het gezin zijn en die informatie aanwenden om de houders van de smart tv's gericht te benaderen met aanbiedingen, bijvoorbeeld met korting op bepaalde *video on demand*.

Niet doorslaggevend is of TP Vision de bedoeling heeft om de individuele betrokkenen te benaderen voor (direct) marketing- en profileringsdoeleinden.
Er is al sprake van een persoonsgegeven wanneer het gegeven voor een op de persoon gericht doel kan worden gebruikt[241], en die mogelijkheid is aanwezig. TP Vision beschikt, zoals aangegeven, bijvoorbeeld over een overzicht van bekeken uitzendingen en het bezoek aan en gebruik van apps, websites in combinatie met meerdere unieke klant- en toestelidentifiers en heeft van alle betrokkenen die gebruik maken van de onlinebetalingsmogelijkheden van MPP Global de naam en adresgegevens, bankrekeningnummers en betalingsgegevens (inclusief type betaling en datum van aankoop) (zie p. 32 van dit rapport).

Daarnaast kan TP Vision betrokkenen benaderen per e-mail (via een hostmailing door Philips) en rechtstreeks per e-mail en per sms (via MPP Global).

Via Philips kan TP Vision ook inzage krijgen in de NAW-gegevens van betrokkenen voor profileringsdoeleinden (zie p. 29 en ook p. 58 van dit rapport).

De gegevens zijn voor TP Vision dan wel enig ander persoon in elk geval in de navolgende gevallen direct dan wel indirect herleidbaar naar identificeerbare natuurlijke personen (gebruikers van de Philips smart tv).

TP Vision beschikt (in ieder geval via de IP-EPG-logbestanden) over de IP-adressen waarmee de smart tv aan internet is verbonden. Bij de internetserviceprovider zijn de IP-adressen gekoppeld aan NAW-gegevens. Deze NAW-gegevens kunnen via een gerechtelijk bevel aan TP Vision of bijvoorbeeld aan opsporingsinstanties verstrekt

[241] Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

worden. De IP-adressen zijn daarom herleidbaar naar identificeerbare natuurlijke personen.[242]

> TP Vision bestrijdt in haar **zienswijze** de conclusie van het CBP dat IP-adressen persoonsgegevens zijn, omdat ze zonder aanvullende identificerende gegevens niet herleidbaar zijn naar een identificeerbare natuurlijke persoon.[243] Volgens TP Vision zijn IP adressen in feite 'gecodeerde gegevens' als bedoeld in de memorie van toelichting bij de Wbp[244], en beschikt TP Vision niet "*over de middelen om zonder veel moeite de tenaamstelling en adresgegevens behorend bij een IP nummer te achterhalen.*"[245]
>
> Onder verwijzing naar CBP-richtsnoeren[246], eerdere beoordelingen door het CBP zelf[247], opinies van de Artikel 29-werkgroep[248] en het (al geciteerde) arrest van het Europees Hof van Justitie, is het uitgangspunt dat IP-adressen in beginsel persoonsgegevens zijn (met uitzondering van IP-adressen die in gebruik zijn door bijvoorbeeld servers). Het CBP wijst op het feit dat de definitie van persoonsgegevens niet alleen herleidbaarheid omvat door de verantwoordelijke zelf, maar ook door een derde. Omdat ISP's de IP-adressen kunnen herleiden naar natuurlijke personen, is er de facto sprake van identificeerbare gegevens, en omdat de gegevens ook door de politie opgevraagd kunnen worden ten behoeve van de opsporing, dienen ze als persoonsgegevens te worden beschouwd. Het gaat bij TP Vision bovendien niet over een verzameling losse IP-adressen op zichzelf, maar om gegevens in onderlinge combinatie of in samenhang met gegevens over individueel kijkgedrag, websitebezoek en appgebruik die direct dan wel indirect –

---

[242] Zie HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), r.o. 26 over de status van IP-adressen, die persoonsgegevens vormen.
[243] Zienswijze TP Vision van 5 april 2013, p. 3.
[244] "Een gegeven is geen persoonsgegeven indien doeltreffende maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Deze maatregelen kunnen bijvoorbeeld zijn gegevenscodering in combinatie met nadere bewerkingen of bijzondere besluitvormingsprocedures. Een verantwoordelijke kan bij voorbeeld gegevens ontdoen van de direct identificerende gegevens en deze onderbrengen bij een derde dan wel een derde de sleutel geven die toegang geeft tot deze gegevens. De vraag of in een dergelijk geval al dan niet gesproken kan worden van persoonsgegevens is afhankelijk van de mate waarin medewerking van de betrokken derde verwacht mag worden. Indien bijvoorbeeld degene die de code heeft opgesteld is onderworpen aan een geheimhoudingsplicht die naar uit de praktijk is gebleken daadwerkelijk wordt gehandhaafd, kan in de regel ervan worden uitgegaan dat er onvoldoende feitelijke mogelijkheden zijn tot daadwerkelijke identificatie. Is de code echter zonder veel moeite of met eenvoudige omzeiling van waarborgen te verkrijgen door de verantwoordelijke, dan is er sprake van identificeerbaarheid en dus van persoonsgegevens in de zin van het wetsvoorstel. De feitelijke situatie, niet de juridische constructie, is bepalend voor de toepasselijkheid van het wetsvoorstel."
[245] Zienswijze TP Vision van 5 april 2013, p. 4.
[246] Publicatie van persoonsgegevens op internet, CBP Richtsnoeren, december 2007, Staatscourant 2007, nr. 240, blz. 10
[247] CBP, z2008-01174, 27 oktober 2008, p. 7-8, URL: http://www.cbpweb.nl/downloads_pb/pb_20081031_geencommentaar.pdf
[248] Artikel 29-werkgroep 136. Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, p. 16-17.

redelijkerwijs, zonder onevenredige inspanning[249] – herleidbaar zijn tot een identificeerbare natuurlijke persoon. De stelling dat het bij IP-adressen om gecodeerde gegevens zou gaan, kan het CBP evenmin onderschrijven. Het gaat hier niet om gegevens die door of in opdracht van een verantwoordelijke zijn ontdaan van identificerende gegevens dan wel versleuteld, en al evenmin om bescherming tegen ontsleuteling via een beroepsgeheim.

Omdat bij het aanzetten van het toestel automatisch Google Analytics-cookies worden geplaatst en gelezen, kan TP Vision, in combinatie met de gegevens die zij via het Service Platform verzamelt, per gebruiker het bezoek aan meerdere websites en gebruik van apps door de tijd heen volgen en opslaan. Conform het rechtsvermoeden in artikel 11.7a van de Tw zijn dit persoonsgegevens. Voor Google zijn deze gegevens op zichzelf persoonsgegevens. De toegepaste maskering van het laatste octet van het IP-adres leidt weliswaar tot verminderde herleidbaarheid (een groep van maximaal 254 verschillende gebruikers), maar er is, door de aanwezigheid van bijkomende gegevens als tijdstip en URL-referrers, gedurende de verzameling van de gegevens door Google, geen onevenredige inspanning nodig om het surfgedrag en appgebruik tot een individuele betrokkene te herleiden.[250]

In haar **zienswijze** betwist TP Vision dat de gebruikte Google Analytics cookies *tracking cookies* zijn. Daardoor zou het rechtsvermoeden uit artikel 11.7a, eerste lid, onder b, van de Tw dat dit persoonsgegevens zijn, niet van toepassing zijn. Dit omdat de code uitsluitend op de webpagina van de App Gallery in het Service Portal is geïmplementeerd, en er dus slechts sprake is van één dienst van de informatiemaatschappij. "*Doordat TP Vision IP-masking heeft ingesteld wordt het laatste byte (of 'octet') van het IP adres dat Google ontvangt automatisch verwijderd voordat Google dit opslaat. Omdat TP Vision tevens de optie van 'gegevens delen' heeft uitstaan, worden de opgeslagen gegevens van televisies door Google uitsluitend gebruikt ten behoeve van de levering van Google Analytics rapporten aan TP Vision.*"[251] De cookies zouden *first party* zijn, en niet *third party*. (zie ook p. 34-35 van dit rapport).

Het CBP reageert hierop als volgt. In tegenstelling tot houders van websites die gebruikmaken van de Google Analytics-dienst op hun eigen website, en daarmee niet zelf het gedrag van gebruikers over andere websites kunnen volgen, heeft TP Vision de dienst zodanig geïmplementeerd dat zij in staat is

[249] In de wetsgeschiedenis bij de Wbp wordt over het begrip 'onevenredige inspanning' opgemerkt: "Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen." Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.
[250] Zie ook de brief van de Artikel 29-werkgroep aan Google van 26 mei 2010, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf. Vergelijk tevens de conclusies van onderzoek door de gezamenlijke Duitse privacytoezichthouders naar de voorwaarden waaronder Google Analytics rechtmatig kan worden ingezet. Mededeling Datenschutz Hamburg, 'Beanstandungsfreier Betrieb von Google Analytics ab sofort möglich', 15 september 2011, URL: http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html
[251] Idem, p. 5.

het klikgedrag van gebruikers op de verschillende apps in de App Gallery te volgen. Deze apps zijn allemaal afzonderlijke diensten van de informatiemaatschappij als bedoeld in artikel 11.7a van de Telecommunicatiewet. Het betreft daarom wel degelijk *tracking cookies* in juridische zin, zoals ook toegelicht in de opinie van de Artikel 29-werkgroep over toestemming voor cookies.[252] Bovendien zijn het juridisch wel degelijk *third party* cookies. Technisch gezien kan weliswaar sprake zijn van cookies die onder het eigen domein van TP Vision worden geplaatst (via haar bewerker IBM), maar juridisch gezien is Google wel degelijk een derde partij die de gegevens over het app-klikgedrag van houders van Philips smart tv's verzamelt en verwerkt (waaronder de toegepaste methode om het laatste octet van het IP-adres na verzameling te verwijderen).[253]

TP Vision beschikt daarnaast over NAW-gegevens van betrokkenen die gebruikmaken van de onlinebetaalmogelijkheden, in combinatie met het Device ID. Omdat het Consumer ID gekoppeld is aan het Device ID, en TP Vision inzage kan krijgen in de NAW-gegevens van betrokkenen, zijn daarom beide gegevens herleidbaar naar identificeerbare natuurlijke personen.

Hoewel TP Vision heeft verklaard geen registratiegegevens te ontvangen van Philips en dit ook is bepaald in de licentieovereenkomst tussen TP Vision en Philips (zie p. 28 van dit rapport), kan TP Vision wel degelijk inzage krijgen in de NAW-gegevens die horen bij het Consumer ID (en bij Philips berusten), met een beroep op de marketingclausule in de overeenkomst met Philips. Het feit dat Philips deze inzage tot op heden niet heeft verleend, zoals TP Vision schrijft[254], laat onverlet dat de contractuele mogelijkheid bestaat.

Ook zou TP Vision via een rechterlijke procedure afgifte door Philips kunnen afdwingen van de NAW-gegevens behorend bij een of meerdere Consumer ID's, bijvoorbeeld in het (hypothetische) geval dat TP Vision aansprakelijk gesteld zou worden voor een auteursrechtinbreuk door een of meerdere gebruikers van Philips smart tv's.

Het Consumer ID is een zelfstandig persoonsgegeven omdat het voor Philips (bij alle geregistreerde klanten) rechtstreeks herleidbaar is naar geïdentificeerde natuurlijke personen. Het feit dat TP Vision het systeem zodanig heeft opgezet dat de registratiegegevens bij Philips berusten en dat de gegevens over het kijkgedrag in

[252] Artikel 29-werkgroep Opinie 04/2012 on Cookie Consent Exemption (juni 2012), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.
[253] Het CBP heeft bovenstaande toepassing van de begrippen 'tracking cookies' en 'third party' voorgelegd aan de ACM in het kader van het Samenwerkingsprotocol CBP-OPTA van beide toezichthouders. De ACM stemt in met de voorgelegde toepassing van deze begrippen in dit rapport.
[254] Brief TP Vision van 8 mei 2013, p. 3.

beginsel gescheiden worden gehouden van de registratiegegevens, leidt niet tot de conclusie dat er geen sprake is van persoonsgegevens.[255]

Aanvullend registreert TP Vision een nieuw uniek nummer (het Mobile Device ID) als de gebruiker de afstandsbedieningsapp gebruikt. Daarbij registreert TP Vision de naam van diens mobiele apparaat. In eerder onderzoek (naar het verzamelen van gegevens over Wifi-routers) heeft het CBP vastgesteld dat deze naam een persoonsgegeven is als mensen hun volledige eigen naam gebruiken en die naam voldoende uniek is, maar zeker in combinatie met andere persoonsgegevens zoals het IP-adres.[256]

Daar komt bij dat TP Vision over de NAW-gegevens van betrokkenen beschikt als zij zich aanmelden bij MPP Global om gebruik te maken onlinebetalingsmogelijkheden (mogelijk sinds 29 oktober 2012). In dat geval heeft TP Vision via haar bewerker MPP Global inzage in diens naam, adres, woonplaats, bankrekeningnummer en betalings- en transactiegegevens, gekoppeld aan het Device ID. In sommige gevallen komt TP Vision ook nog te beschikken over NAW-gegevens van betrokkenen, in geval zij contact opnemen met de servicedesk en er een monteur heen gestuurd moet worden.

Identificatie kan ook plaatsvinden zonder dat de naam van de betrokkene wordt achterhaald, zoals ook WP29 toelicht in zijn advies over persoonsgegevens.[257] Vereist is slechts dat de betrokkene aan de hand van de beschikbare informatie in combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) van andere personen kan worden onderscheiden.

Uit de overeenkomsten met Philips, Gracenote, MPP Global en uit de verklaringen van TP Vision (inclusief de oude en nieuwe privacystatements en de cookiepolicy) blijkt dat TP Vision de betrokkenen gericht kan en wil benaderen.

De recommenderdienst van Gracenote is gebaseerd op analyse van het historische onlinekijkgedrag en leidt tot gerichte aanbevelingen voor uitzendingen, gebaseerd op een profiel van de betrokkene. Het doeleinde van de verwerking is er dus mede erop gericht om individuele betrokkenen te kunnen onderscheiden en te benaderen.
Via MPP Global kan TP Vision (segmenten van) betrokkenen benaderen per e-mail en per sms. Via Philips kan TP Vision inzage krijgen in de registratiegegevens om consumentenprofielen op te stellen en kan TP Vision betrokkenen e-mailen.

Het CBP neemt daarbij in aanmerking dat de verwerking van de gegevens volgens TP Vision mede voor de volgende doeleinden geschiedt:

---

[255] Wel zal het feit dat identificatiebeperkende maatregelen zijn genomen een positieve rol spelen bij een beoordeling of is voldaan aan de beveiligingsverplichting van artikel 13 van de Wbp, maar de getroffen beveiligingsmaatregelen vallen buiten de scope van dit onderzoek door het CBP.
[256] Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010 (z2010-00582), p. 34 e.v.
[257] Zie voetnoot 19.

- het verbeteren van de advertentie-ervaring;
- het leveren van kijkaanbevelingen op basis van kijkgedrag;
- het verlenen van kortingscontent of gratis content door applicatieaanbieders aan consumenten;
- het verstrekken van gegevens aan politie en justitie op grond van een bevoegd gegeven last of vordering of op basis van een andere wettelijke verplichting.

Gegevensverwerkingen voor deze doeleinden hebben slechts nut als die het mogelijk maken specifieke personen te identificeren. Om deze doeleinden te verwezenlijken moeten de verwerkte gegevens herleidbaar zijn tot de betrokken abonnees. De gegevensverwerking is (dan) mede gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens, conform het advies over persoonsgegevens van de Artikel 29-werkgroep.

Het verweer van TP Vision dat zij alleen anonieme productprofielen bijhoudt, niet op naam van een individuele consument, laat onverlet dat zij over de mogelijkheid beschikt en technisch in staat moet worden geacht (onder meer omdat het Consumer/Device ID als centraal koppelpunt in de databases fungeert) om gedetailleerde profielen op te stellen van betrokkenen op grond van hun onlinekijk- en internetgedrag via de Philips smart tv en deze profielen in de praktijk op betrokkenen toe te passen, door hen te benaderen met gerichte aanbiedingen.

In haar zienswijze op het rapport voorlopige bevindingen heeft TP Vision verklaard dat het softwareplatform waar Smart TV op draait, per televisie wordt ingericht en niet per toeschouwer of gebruiker. "*Er zijn geen aparte inlog-codes of inlog-profielen per individuele gebruiker (zoals dat bijvoorbeeld bij een computer operating systeem als Microsoft Windows wel het geval is of kan zijn), waardoor niet zondermeer kan worden nagegaan welke persoon nu precies gebruik maakt van de televisie of de Smart TV functionaliteiten. De notie dat gegevens die door de individuele televisie met (de servers van) TP Vision (of haar leveranciers zoals IBM) worden gedeeld per definitie herleidbaar zijn tot een specifiek identificeerbare natuurlijke persoon is daarom niet altijd correct. TP Vision weet niet wie er voor de televisie zit en een televisie kan worden gebruikt door een huishouden met een vader, moeder en twee kinderen, maar kan ook in een studentenhuis met 14 bewoners staan. In een groot aantal gevallen (met meer dan 1 potentiële tv kijker) zullen de door TP Vision opgeslagen gegevens dan ook, al dan niet via bewerkelijke omwegen, hoogstens (in geaggregeerde vorm) per huishouden kunnen worden vastgesteld.*"[258]

Dat een televisie door meerdere personen in een huishouden kan worden gebruikt, laat onverlet dat het wel degelijk om persoonsgegevens gaat.

Een vaste telefoon kan ook door meerdere personen in het huishouden worden gebruikt. Dit geldt ook voor bijvoorbeeld een auto. Dit staat, ook volgens de parlementaire geschiedenis van de Wbp[259], niet in de weg aan de conclusie dat het een

[258] Zienswijze TP Vision van 5 april 2013, p. 2.
[259] Kamerstukken II, 1997/98, 25 892, nr. 9, p. 2. "Aannemelijk is immers dat een zodanig gebruik van het gegeven consequenties heeft of kan hebben voor de persoon met wie het telefoonnummer in

persoonsgegeven betreft als de gegevens over het gebruik aan de houder van de telefoon of auto worden toegerekend. In veel gevallen beschikt TP Vision over de registratiegegevens van de houder van het toestel, als die zich heeft geregistreerd om onlinefilms en -video's te kunnen kopen via MPP Global, of indirect, via Philips.

Het verweer van TP Vision dat geen sprake zou zijn van persoonsgegevens is bovendien in logische tegenspraak met de aard van de gepersonaliseerde dienstverlening. Het feit dat TP Vision een gepersonaliseerde recommenderdienst aanbiedt, geeft aan dat individuele personen in het huishouden kennelijk effectief benaderd, en anders behandeld kunnen worden zonder hun individuele namen te kennen. Indien de recommenderdienst voortdurend programma's zou aanbevelen die gebaseerd zijn op het kijkgedrag van een 'andere' persoon, met hele andere interesses, zou het nut van de recommenderdienst beperkt zijn. In de praktijk valt het onderscheid eenvoudig te maken naar het tijdstip van de dag waarop gekeken wordt. Kort samengevat: 's ochtends kunnen andere aanbevelingen (en advertenties) worden getoond dan ’s middags, na het uitgaan van de scholen, en 's avonds. Bovendien kan uit het kijkgedrag informatie worden afgeleid over de gezinssituatie (aanwezigheid van bijvoorbeeld kinderen), waarmee de beslisser in het huishouden gericht benaderd kan worden. Via de recommenderdienst worden de gevolgen van het kijken door meerdere personen dus effectief toegerekend aan de houder van het toestel.[260]

Ten aanzien van het door TP Vision genoemde voorbeeld van het studentenhuis acht het CBP herleidbaarheid overigens ook mogelijk. Als een van de studenten via *video on demand* bijvoorbeeld een film bestelt, zal dat op de eindafrekening zichtbaar worden, en zal degene die de facto de rekening betaalt, de werkelijke kijker kunnen en willen identificeren.

Ten overvloede merkt het CBP op dat van de 7,51 miljoen huishoudens in Nederland begin 2012 inmiddels bijna 40 procent een eenpersoonshuishouden is (2,76 miljoen) en dat dat aantal de komende jaren nog toeneemt.[261]

---

verband is gebracht. Een hiermee tot op zekere hoogte vergelijkbare situatie kan zich voordoen bij het gebruik van kentekens van auto's."

[260] Zie bijvoorbeeld: Thorsten Hennig-Thurau, André Marchand en Paul Marx, 'Can Automated Group Recommender Systems Help Consumers Make Better Choices?', Journal of Marketing Volume 76 (September 2012), 89 –109, p. 90. URL: http://www.marketingcenter.de/lmm/research/publications/download/Hennig-Thurau_Marchand_Marx_JM_2012.pdf. "In both practice and research, most automated recommenders focus on an individual consumer’s preferences, ignoring a common consumption situation for hedonic products and services— namely, joint consumption by a group of consumers." En: "Moreover, although consumption takes place jointly, often only a fraction of the group members participates in the actual decision-making process, acting as agents for the other members (Weinberg 2003)."

[261] CBS, PBL, Wageningen UR (2013). Bevolkingsomvang en aantal huishoudens, 1980-2013 (indicator 0001, versie 14, 23 april 2013).URL: http://www.compendiumvoordeleefomgeving.nl/indicatoren/nl0001-Bevolkingsomvang-en-huishoudens.html?i=15-12

Gelet op het voorgaande zijn de in deze paragraaf genoemde gegevens die samenhangen met en voortvloeien uit het gebruik van de Philips smart tv persoonsgegevens.

3.3 Verwerking van persoonsgegevens

In de vorige paragraaf is vastgesteld welke gegevens die met of door een Philips smart tv worden gegenereerd en/of vastgelegd persoonsgegevens zijn. TP Vision is hiervoor verantwoordelijk omdat zij de feitelijke macht heeft over deze gegevens. TP Vision verzamelt (en laat verzamelen door andere partijen in haar opdracht), legt vast, bewaart, raadpleegt en analyseert de persoonsgegevens die samenhangen met en voortvloeien uit het gebruik van de Philips smart tv, en brengt deze samen en met elkaar in verband onder meer voor het gebruik van deze gegevens om persoonlijke kijkaanbevelingen te doen (de recommenderdienst), om in de nabije toekomst gerichte advertenties te kunnen tonen en voor de inventarisatie en statistische analyse van het gebruik van de Philips smart tv, inclusief bekeken uitzendingen, gehuurde films (*video on demand*), gebruik van apps en bezoek aan websites.

Gelet op het voorgaande verwerkt TP Vision persoonsgegevens.

3.4 Bewerkersovereenkomst

TP Vision maakt gebruik van de diensten van vijf verschillende bedrijven.

Akamai
Het CBP heeft in paragraaf 2.2.2 vastgesteld dat TP Vision via IBM gebruikmaakt van de diensten van Akamai, en dat Akamai een subbewerker is van IBM.

Naar aanleiding van het onderzoek heeft TP Vision de overeenkomst met IBM ten aanzien van subbewerkers aangepast. De beoordeling van deze overeenkomst komt aan de orde onder het kopje "IBM" (zie p. 64 van dit rapport).

Google Analytics
Het CBP heeft in paragraaf 2.2.2, onder het kopje 'Google Analytics' (p. 34-35 van dit rapport) vastgesteld dat TP Vision gebruikmaakt van de diensten van Google Analytics. In paragraaf 3.2 is vastgesteld dat de gegevens die TP Vision verwerkt, persoonsgegevens zijn, zowel voor TP Vision als voor Google.

TP Vision heeft verklaard de standaard terms en conditions van Google te hebben ondertekend voor het gebruik van Google Analytics en geen aparte bewerkersovereenkomst te hebben gesloten met Google.[262] Google heeft schriftelijk geweigerd een bewerkersovereenkomst te sluiten met TP Vision.

[262] In haar schriftelijke beantwoording van 16 januari 2013 heeft TP Vision verklaard dat het Googleaccount door een werknemer van TP Vision is geopend en dat deze werknemer dit account namens TP Vision beheert.

De standaard terms en conditions van Google kwalificeren niet als een bewerkersovereenkomst of vergelijkbare rechtshandeling die betrekking heeft op de bescherming van persoonsgegevens in de zin van artikel 14, tweede lid, van de Wbp. De overeenkomst moet naar zijn aard betrekking hebben op de gegevensverwerking. De overeenkomst mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is. Daarvan is in casu sprake. De verplichtingen moeten over en weer bovendien duidelijk zijn neergelegd en de overeenkomst moet op dat punt voldoende gedetailleerd zijn. Uitgangspunt daarbij is dat de bewerker daadwerkelijk op instructie van de verantwoordelijke kan handelen. Aan deze vereisten van een bewerkersovereenkomst voldoen bovengenoemde algemene voorwaarden niet.

Dat Google zich op het standpunt stelt dat geen sprake is van persoonsgegevens laat onverlet dat op TP Vision de verplichting rust een bewerkersovereenkomst te sluiten indien zij persoonsgegevens laat verwerken door een derde partij. Door het ontbreken van een bewerkersovereenkomst met Google handelt TP Vision in strijd met het bepaalde in artikel 14, tweede lid, van de Wbp.

Gracenote

Het CBP heeft in paragraaf 2.2.2, onder het kopje 'Gracenote' (p. 29 e.v. van dit rapport) vastgesteld dat TP Vision gebruikmaakt van de diensten van Gracenote. Naar aanleiding van het onderzoek heeft TP Vision zowel standard contractual clauses afgesloten met Gracenote (de EU-modelcontractbepalingen verantwoordelijke-bewerker) als (per 6 mei 2013) een aparte bewerkersovereenkomst naar Nederlands recht.

Het CBP stelt vast dat de eerste overeenkomst overeenkomt met de modelcontractbepalingen 2010/87/EU van de Europese Commissie.[263] Dit (model)contract wordt gebruikt in het kader van doorgifte van persoonsgegevens naar verwerkers van persoonsgegevens gevestigd in landen buiten de EU en ziet op het bieden van algemeen aanvaarde passende waarborgen die noodzakelijk zijn in geval van doorgifte.[264]

Daarnaast hebben partijen een bewerkersovereenkomst gesloten naar Nederlands recht. Het CBP heeft vastgesteld dat uit de overeenkomst specifiek en uitgebreid blijkt wat onder meer de doeleinden van en de middelen voor de verwerking van persoonsgegevens zijn, alsmede het gebruik dat van de gegevens wordt gemaakt, inclusief bewaartermijnen. De overeenkomst voldoet daarmee aan de verschillende vereisten die gesteld worden aan een bewerkersovereenkomst zoals genoemd in paragraaf 2.1.4 van dit rapport.

[263] Commission Decision of 5 february 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.
[264] Naleving van het bepaalde in artikel 76 e.v. van de Wbp (doorgifte) valt buiten de scope van dit onderzoek door het CBP.

Gelet op het bovenstaande voldoet TP Vision sinds 6 mei 2013 aan de bepalingen van artikel 14, tweede lid, van de Wbp voor wat betreft het opstellen van een bewerkersovereenkomst met bewerker Gracenote. Hierdoor handelt TP Vision op dit punt niet langer in strijd met het bepaalde in artikel 14 van de Wbp.

IBM
Het CBP heeft in paragraaf 2.2.2, onder het kopje 'IBM' (p. 30 e.v. van dit rapport) vastgesteld dat TP Vision gebruikmaakt van de diensten van IBM.

Op 13 juli 2012 hebben TP Vision en IBM een Service Agreement gesloten.[265]
Deze overeenkomst kwalificeert niet als een bewerkersovereenkomst in de zin van artikel 14, tweede lid, van de Wbp. De overeenkomst moet naar zijn aard betrekking hebben op de gegevensverwerking. De overeenkomst mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is. Daarvan is in casu sprake. De verplichtingen moeten over en weer bovendien duidelijk zijn neergelegd en de overeenkomst moet op dat punt voldoende gedetailleerd zijn. Aan deze vereisten van een bewerkersovereenkomst voldoet dit Service Agreement niet.

Naar aanleiding van het onderzoek heeft TP Vision een bewerkersovereenkomst gesloten met IBM (ondertekend op 6 mei 2013). De overeenkomst bevat (onder meer) de verplichtingen die IBM als bewerker op zich neemt naar Nederlands recht. Het CBP heeft vastgesteld in paragraaf 2.2.2 van dit rapport, onder het kopje 'IBM', dat uit de overeenkomst specifiek en uitgebreid blijkt wat onder meer de doeleinden van en de middelen voor de verwerking van persoonsgegevens zijn, alsmede het gebruik dat van de gegevens wordt gemaakt, inclusief bewaartermijnen. De overeenkomst voldoet daarmee aan de verschillende vereisten die gesteld worden aan een bewerkersovereenkomst zoals genoemd in paragraaf 2.1.4 van dit rapport.

Bovendien bevat de overeenkomst adequate bepalingen over subbewerkerschap. Uit de overeenkomst blijkt dat TP Vision IBM ruimte laat delen van de verwerking uit te besteden aan subbewerkers. Meer specifiek is bepaald dat de subbewerker zich moet richten naar instructies van TP Vision en de bewerker IBM, de subbewerker bepaalde beveiligingsmaatregelen moet implementeren alsmede tot geheimhouding verplicht is. Daartoe zal IBM nog een specifieke overeenkomst sluiten met de betreffende subbewerker.

Gelet op het bovenstaande voldoet TP Vision sinds 6 mei 2013 aan de bepalingen van artikel 14, tweede lid, van de Wbp voor wat betreft het opstellen van een bewerkersovereenkomst met bewerker IBM, inclusief de relatie met subbewerker Akamai. Hierdoor handelt TP Vision op dit punt niet langer in strijd met het bepaalde in artikel 14 van de Wbp.

[265] Global Process Services, Consumer Electronics Service Delivery Platform, Service Agreement d.d. 13 juli 2012, ondertekend door TP Vision Netherlands B.V. en IBM Nederland B.V.

MPP Global

Het CBP heeft in paragraaf 2.2.2, onder het kopje 'MPP Global' (p. 32 e.v. van dit rapport) vastgesteld dat TP Vision gebruikmaakt van de diensten van MPP Global. Naar aanleiding van het onderzoek heeft TP Vision op 30 december 2012 een voorstel gedaan aan MPP Global tot het aangaan van een bewerkersovereenkomst. De overeenkomst is op 5 februari 2013 door partijen ondertekend.

De overeenkomst bevat (onder meer) de verplichtingen die MPP Global als bewerker op zich neemt naar Engels recht. Zo heeft de overeenkomst naar zijn aard betrekking op de gegevensverwerking, zijn in Annex 2 de te treffen technische en organisatorische beveiligingsmaatregelen opgenomen en bevat de overeenkomst bepalingen over onder meer de mate van zeggenschap van de bewerker, het gebruik van de gegevens, audit en opslag van de gegevens. In combinatie met het bepaalde in de onderliggende Outsourcing Agreement, voldoet de overeenkomst daarmee aan de verschillende vereisten die gesteld worden aan een bewerkersovereenkomst zoals genoemd in paragraaf 2.1.4 van dit rapport.

Gelet op het bovenstaande voldoet TP Vision sinds 6 februari 2013 aan de bepalingen van artikel 14, tweede lid, van de Wbp voor wat betreft het opstellen van een bewerkersovereenkomst met bewerker MPP Global. Hierdoor handelt TP Vision op dit punt niet langer in strijd met het bepaalde in artikel 14 van de Wbp.

3.5 Informatieplicht

Het CBP heeft in paragraaf 2.2.2 van dit rapport vastgesteld dat TP Vision cookies plaatst en informatie uitleest van de Philips smart tv's. Dit betekent dat TP Vision ter zake moet voldoen aan de informatieverplichting uit artikel 11.7a, eerste lid, onder a, van de Tw. TP Vision dient de gebruikers van de tv's te informeren voorafgaand aan het plaatsen van cookies. De informatie moet duidelijk en volledig zijn, overeenkomstig de Wet bescherming persoonsgegevens en in ieder geval zien op de doeleinden waarvoor de informatie wordt geplaatst en gelezen.

Het CBP heeft in de paragrafen 3.2 en 3.3 van dit rapport vastgesteld dat TP Vision persoonsgegevens verwerkt over het onlinekijk- en internetgedrag van betrokkenen.

Dit betekent dat TP Vision ook los van het bepaalde in de Tw moet voldoen aan de verplichtingen uit artikel 33 jo. 34 Wbp (informatieplicht). TP Vision dient vóór het moment van de verkrijging van de persoonsgegevens haar identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mede te delen en nadere informatie te verstrekken over bijvoorbeeld de categorieën van verwerkte persoonsgegevens en de bewaartermijn, voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.[266]

[266] Vgl. Last onder dwangsom NS Groep N.V. CBP 9 juni 2011, z2011-00057. URL: http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_NS.pdf

Ten aanzien van het mededelen van haar identiteit in de zin van deze artikelen 33 jo. 34 van de Wbp, geldt het volgende.

Toen het CBP zijn onderzoek instelde, bevatte de op consumenten gerichte websites van Philips geen informatie over de rol en verantwoordelijkheid van TP Vision bij het gebruik van een Philips smart tv. De eigen website van TP Vision bevatte een summier privacystatement dat alleen zag op de gegevensverwerking van bezoekers van die website en het verwerken van gegevens van sollicitanten of gegevens van overgekochte bedrijven. Ook de verpakking van de tv bevat geen informatie over TP Vision. Pas na eerste installatie kan een betrokkene op het scherm informatie lezen over gegevensverwerking via de tv, maar hier werd en wordt als identiteit van de verantwoordelijke de naam 'Net_TV' gebruikt.

Ten aanzien van het mededelen van nadere informatie in de zin van de artikelen 33 jo. 34 van de Wbp, geldt het volgende.

Gebruikers van een Philips smart tv werden tot medio oktober 2012 niet geïnformeerd wie TP Vision was, dat er cookies worden geplaatst en uitgelezen door TP Vision en haar bewerkers, welke gegevens er via de cookies en anderszins via de televisie worden geregistreerd en verwerkt en hoe lang deze gegevens werden bewaard. TP Vision had dat ook niet gemeld bij het CBP, noch was deze informatie op andere wijze kenbaar gemaakt.

Na aanvang van het onderzoek door het CBP heeft TP Vision de Net_TV Gebruiksvoorwaarden herzien en uitgebreid met een privacyparagraaf, en daarnaast (voor het eerst) een Privacy Statement gemaakt en een aparte cookieverklaring.

In haar melding bij het CBP en in haar Privacy Statement en de Cookie Policy geeft TP Vision relevante nadere informatie over haar identiteit, haar bewerkers en de aard en omvang van de gegevensverwerking, inclusief het plaatsen en uitlezen van informatie met behulp van cookies. TP Vision gaf hierin echter geen informatie over de bewaartermijn(en). Gezien het gevoelige karakter van de informatie over het onlinekijkgedrag, appgebruik en websitebezoek, en het gebruik dat hiervan wordt gemaakt (ten behoeve van de recommenderdienst) dient TP Vision deze informatie wel te verstrekken aan betrokkenen.

Deze informatie over de gegevensverwerking dient publiek beschikbaar en toegankelijk te zijn vóórdat er gegevens worden verwerkt. Het ligt voor de hand, zeker in dit geval waarbij gegevensverwerking via internet een grote rol speelt, om dergelijke informatie in een onlineprivacyverklaring te vermelden. Artikel 33 en 34 van de Wbp gaan er vanuit dat er geen onderzoeksplicht van de betrokkene is. Transparantie over de gegevensverwerking is essentieel om betrokkenen in staat te stellen een weloverwogen keuze te maken met betrekking tot hun persoonsgegevens en persoonlijke levenssfeer.

Deze transparantie ontbreekt. Sinds begin oktober 2012 stelt TP Vision weliswaar de gebruiksvoorwaarden, het Privacy Statement en de Cookie Policy in het

Nederlands beschikbaar op de publiek toegankelijke URL's op het hoofddomein tou.nettvservices.com, maar deze URL's waren niet gelinkt vanaf de relevante Philips- en TP Vision-consumentenwebsites en evenmin te vinden via zoekmachines. Ook anderszins werden en worden potentiële kopers niet geïnformeerd over de gegevensverwerkingen via de toestellen.

TP Vision heeft naar aanleiding van het Rapport voorlopige bevindingen van het CBP maatregelen getroffen om haar zichtbaarheid te vergroten, bijvoorbeeld door het Privacy Statement en de Cookie Policy op de website www.tpvision.com te plaatsen en door een vraag en antwoord over privacy toe te laten voegen aan een webpagina van Philips over een specifieke smart tv. Bovendien heeft TP Vision aan het Privacy Statement en de Cookie Policy informatie toegevoegd over haar bewerkers en de bewaartermijnen van de verschillende gegevens.

Deze maatregelen zijn echter onvoldoende. Het CBP heeft vastgesteld dat het nieuwe Privacy Statement en de Cookie Policy (van 1 mei 2013) alleen in het Engels beschikbaar zijn. Het CBP heeft tevens vastgesteld (zie p. 44 van dit rapport) dat de verklaringen niet of onvoldoende publiek toegankelijk zijn, niet via de eigen website(s) van TP Vision en niet via zoekmachines.

Pas na aanschaf, bij eerste installatie, kan een betrokkene op het scherm in de gebruiksvoorwaarden informatie lezen over de gegevensverwerking. Op dat moment heeft de betrokkene er in veel gevallen al voor gekozen om de televisie op internet aan te sluiten, en is de gegevensverwerking dus al begonnen. De informatie op het scherm komt dus te laat om de betrokkenen in staat te stellen een weloverwogen keuze te maken.[267] Daar komt bij dat het ruim tien minuten duurt voordat de algemene voorwaarden, het privacy en cookiebeleid volledig getoond zijn (door een automatische scroll).[268] Dit lijkt een te hoge eis te stellen aan het geduld van betrokkenen. Daarom is de wijze waarop deze informatie wordt verstrekt, niet adequaat. Het CBP heeft bovendien vastgesteld dat de URL die gebruikers op het scherm zien bij eerste installatie, als zij meer willen lezen over het privacybeleid, sinds 18 april 2013 (voor nieuwe gebruikers) respectievelijk 2 juni 2013 (voor bestaande gebruikers) niet langer functioneel is (omdat die nog naar het oude domein tou.nettvservices.com verwijst).

Het gebrek aan zeggenschap door het ontbreken van nadere informatie deed en doet zich met name voor bij verdere ingebruikname van het toestel, als de betrokkene gebruik wil maken van de onlinediensten. De betrokkene zal dan in veel gevallen eerst de tv-gids activeren, en moet dan de algemene voorwaarden van Gracenote accepteren. Deze voorwaarden bevatten in het geheel geen informatie over de gegevensverwerking. Tot 18 april 2013 (voor nieuwe gebruikers) respectievelijk 2 juni 2013 (voor bestaande gebruikers) verscheen

[267] Dit heeft ook gevolgen voor de keuzevrijheid om toestemming te geven, zoals hieronder besproken op p. 68 e.v. van dit rapport.
[268] Het CBP heeft dit getimed tijdens het eerste controle-onderzoek naar een Philips smart tv op 25 februari 2013 en tijdens het controle-onderzoek op 3 juni 2013. Toen duurde het ruim 15 minuten voor de tekst volledig was getoond.

gedurende 10 seconden een pop-up in beeld over het bestaan van kijktips (de recommender). Deze tekst meldde dat voor de kijktips *wordt uitgegaan van uw eerdere kijkvoorkeuren op dit toestel.* De tekst bevatte geen informatie over het plaatsen en uitlezen van cookies of over de bewaartermijn van de aldus verzamelde gegevens over het onlinekijkgedrag.

Naar aanleiding van het onderzoek heeft TP Vision een toestemmingsvraag ingevoerd voor het registreren van kijkgedrag via cookies (zie hieronder, paragraaf 3.6 van dit rapport). De gebruiker wordt geïnformeerd dat er 'regelmatig' cookies worden geplaatst. Die aanduiding is niet specifiek genoeg. De gebruiker kan hieruit niet opmaken dat dit elke drie tot vijf minuten gebeurt en dat zijn kijkgedrag dus zeer nauwgezet wordt vastgelegd. De tekst bevat geen toelichting op de term 'kijkgedrag'. De gebruiker wordt niet geïnformeerd dat de cookies niet alleen zien op het kijken naar specifieke zenders en programma's, maar ook op het huren van films en bekijken van gemiste uitzendingen. De verwijzing naar 'de Philips TV website' waarop de gebruiker meer informatie zou kunnen lezen, biedt evenmin soelaas. Het CBP heeft op 3 juni 2013 vastgesteld dat het Privacy Statement en de Cookie Policy daar (nog) niet te vinden zijn.

Ook ten aanzien van de optionele registratie bij Philips is de informatie onvoldoende duidelijk. Tot 18 april 2013 (voor nieuwe gebruikers) respectievelijk 2 juni 2013 (voor bestaande gebruikers) suggereerde de tekst op het registratiescherm dat een gebruiker zich moest registreren om software-updates te ontvangen. Het is algemeen bekend dat software-updates van groot belang zijn voor de beveiliging van de persoonsgegevens die op en via het apparaat worden verwerkt. Als dergelijke updates alleen beschikbaar worden gesteld aan klanten die zich hebben geregistreerd, wordt de vrijwilligheid van de registratie ondergraven. TP Vision en Philips maakten onvoldoende duidelijk dat registratie vrijwillig was en dat het apparaat ook zonder registratie naar behoren zou blijven functioneren.

Naar aanleiding van het Rapport voorlopige bevindingen van het CBP heeft TP Vision de tekst in het registratiescherm aangepast. De verwijzing naar software-updates is van dit scherm verwijderd. Tijdens het controle-onderzoek door het CBP bleek echter in de installatie-flow op een ander scherm een advies te verschijnen om te registreren bij Philips voor 'gratis software updates'. Daarmee wordt (opnieuw) ten onrechte gesuggereerd dat gebruikers zich moeten registreren om software-updates te ontvangen.

Door het ontbreken van informatie over haar identiteit en nadere informatie over de gegevensverwerking via de Philips smart tv's (inclusief de rol van bewerkers en het plaatsen en uitlezen van cookies) handelt TP Vision in strijd met artikel 34 Wbp, jo. artikel 11.7a, eerste lid, van de Tw.

Door de wijze waarop TP Vision tijdens het installatieproces gebruikers adviseert om zich te registreren bij Philips, handelt TP Vision (in haar gezamenlijke verantwoordelijkheid met Philips voor deze gegevensverzameling) in strijd met artikel 33 Wbp.

3.6 Grondslag

Het CBP heeft vastgesteld in paragraaf 2.2.2 van dit rapport dat TP Vision en haar bewerkers gegevens plaatsen op en uitlezen van de Philips smart tv's, deels met behulp van cookies. Voor deze cookies dient TP Vision op grond van artikel 11.7a van de Tw geïnformeerde toestemming te vragen.

> Volledigheidshalve merkt het CBP op dat de uitzonderingen in artikel 11.7a van de Tw op het toestemmingsvereiste voor functionele cookies niet van toepassing zijn op de gegevens die Gracenote plaatst en uitleest via het service portal om het onlinekijkgedrag te registreren, op de cookies die Google plaatst om appgebruik in kaart te brengen en op de cookies die in de nabije toekomst voor 'uitgebreidere' advertentiedoeleinden worden geplaatst (door TP Vision en/of door derde partijen). Het plaatsen en uitlezen van deze cookies is immers niet strikt noodzakelijk om gebruik te kunnen maken van de Philips smart tv. De functionaliteit van webstatistieken, advertenties en analyse van het online-appgebruik voldoet evenmin aan het vereiste dat het noodzakelijk is voor een door de gebruiker gevraagde dienst (artikel 11.7a, derde lid, onder b, van de Tw). Wat betreft de analytische cookies geldt dat als het conceptwetsvoorstel tot aanpassing van artikel 11.7a Tw zoals dat in internetconsultatie is gegaan wet wordt, deze cookies – bij ongewijzigde omstandigheden – niet voldoen aan het vereiste dat het plaatsen of lezen van een cookie geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de internetter. Dit omdat TP Vision niet in een bewerkersovereenkomst met Google heeft afgesproken dat ook zij de informatie niet zal gebruiken op een manier die meer dan geringe gevolgen heeft voor de privacy van de internetgebruiker wiens gegevens het betreft.[269]

Het CBP heeft in paragraaf 3.2 van dit rapport vastgesteld dat bij het plaatsen en lezen van de cookies voor het vastleggen van het onlinekijkgedrag en appgebruik en websitebezoek sprake is van een verwerking van persoonsgegevens. Artikel 11.7a van de Tw biedt geen grondslag voor de verwerking van persoonsgegevens. Daarom dient TP Vision niet alleen te voldoen aan het bepaalde in artikel 11.7a van de Tw, maar daarnaast ook een grondslag te hebben voor de gegevensverwerking zoals bepaald in artikel 8 van de Wbp.

Gelet op de samenloop van artikel 8 van de Wbp met artikel 11.7a van de Tw komt daarvoor in de eerste plaats de grondslag ondubbelzinnige toestemming in aanmerking (artikel 8, aanhef en onder a, van de Wbp).[270] Het verschil tussen

---

[269] Het CBP heeft bovenstaande toepassing van de uitzonderingen op het toestemmingsvereiste in artikel 11.7a van de Tw voorgelegd aan de ACM in het kader van het Samenwerkingsprotocol CBP-OPTA van beide toezichthouders. De ACM stemt in met de voorgelegde toepassing van deze uitzonderingen in dit rapport.

[270] Zie bijvoorbeeld Kamerstukken II 2010/2011, 32 549, nr. 39, p. 2. "Los van het toestemmingsvereiste voor het plaatsen en lezen van cookies in artikel 11.7a Tw moet altijd ook nog aan de vereisten in de Wbp worden voldaan indien er bij of door middel van het plaatsen of lezen van cookies persoonsgegevens worden verwerkt. Dit betekent dat in die gevallen op grond van artikel 8 Wbp «ondubbelzinnige» toestemming vereist is (…)."

'toestemming' en 'ondubbelzinnige toestemming' is dat bij de verantwoordelijke elke twijfel moet zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.

Uit de wetsgeschiedenis blijkt dat ook andere grondslagen in aanmerking kunnen komen[271], zoals bijvoorbeeld artikel 8, aanhef en onder f, van de Wbp, dat de gegevensverwerking noodzakelijk is ter behartiging van een gerechtvaardigd belang, mits daarbij het belang van betrokkenen op bescherming van hun persoonlijke levenssfeer niet prevaleert.

Ondubbelzinnige toestemming

Ten aanzien van ondubbelzinnige toestemming geldt het volgende. Van toestemming is, zoals vermeld in paragraaf 2.1.6 (p. 20 e.v. van dit rapport), slechts sprake wanneer er een vrije, specifieke en op informatie berustende wilsuiting is (artikel 1, aanhef en onder i, van de Wbp) waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Het feit dat een betrokkene de algemene voorwaarden (waaronder een beknopte toelichting op het privacybeleid) getoond krijgt bij eerste installatie, en 'ga door' dient te klikken om verder te gaan met de installatie, kwalificeert niet als een vrije wilsuiting. De gebruiker heeft feitelijk geen andere keuze dan de Net_TV Gebruiksvoorwaarden te accepteren. Informatie over het doel van de verwerking mag bovendien niet worden opgenomen in bijvoorbeeld algemene voorwaarden, maar dient gegeven te worden in een afzonderlijke toestemmingsclausule (geen specifieke wilsuiting).[272]

De pop-up die (tot 18 april 2013 voor nieuwe gebruikers, respectievelijk 2 juni 2013 voor bestaande gebruikers) verscheen na het inschakelen van de recommenderdienst waarin wordt gewezen op een opt-outmogelijkheid, kan evenmin worden aangemerkt als toestemming. In het gebruik van de term 'wilsuiting' ligt een actie van de betrokkene besloten (oftewel, instemming en geen opt-out). Uit het uitblijven van een

[271] Zie bijvoorbeeld Kamerstukken I 2011/12, 32 549, E, p. 5-6. "Anders dan enkele leden aannemen, betekent de omstandigheid dat deze handelingen onder de Wbp vallen overigens niet per se dat daarvoor ondubbelzinnige toestemming vereist is. Artikel 8 Wbp noemt naast ondubbelzinninge toestemming van de betrokkene nog vijf andere rechtvaardigingsgronden." Zie ook p. 7: "(…) indien geen sprake is van de overige rechtvaardigingsgronden in artikel 8 Wbp, ondubbelzinnige toestemming van de gebruiker een vereiste moet zijn" en p. 11-12: "(…) dus ondubbelzinnige toestemming hebben verkregen, of een beroep doen op een andere rechtvaardigingsgrond van artikel 8 Wbp." "Ook kan de behartiging van het gerechtvaardigde belang van degene die de gegevens verwerkt een rechtvaardiging vormen voor verwerking van persoonsgegevens, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene (in het bijzonder het recht op bescherming van de persoonlijke levenssfeer) prevaleert. Het is echter niet aannemelijk dat hier snel sprake van zal zijn bij het gebruik van tracking cookies. Om die reden zal op grond van de Wbp over het algemeen 'ondubbelzinnige toestemming' van de betrokkene nodig zijn." Toelichting bij Concept wetsvoorstel met toelichting met betrekking tot artikel 11.7a van de Telecommunicatiewet (cookiebepaling), p. 15. URL: http://internetconsultatie.nl/cookiebepaling.

[272] Artikel 29-werkgroep WP 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 40.

opt-out van de betrokkene (het uitschakelen van 'personalisatie' in het systeemmenu) of het feit dat een betrokkene geen gebruikmaakt van de mogelijkheid om via het systeemmenu cookies te verwijderen, kan TP Vision niet afleiden dat de betrokkene instemt met deze gegevensverwerking (geen 'ondubbelzinnige toestemming').

De (browser van de) Philips smart tv is zodanig ingesteld dat cookies automatisch worden geaccepteerd en dat levert, zoals ook de Artikel 29-werkgroep in haar advies over toestemming heeft bevestigd, geen rechtsgeldige toestemming op (zie paragraaf 2.1.6, p. 20 van dit rapport). Veel browsers, waaronder die van de Philips smart tv, staan standaard ingesteld op het accepteren van alle cookies. Uit het feit dat de gebruiker deze standaardinstelling niet heeft gewijzigd, kan geen toestemming voor het gebruik van cookies worden afgeleid. Het is aan de plaatser van de cookies (de website) om via een vrije, specifieke en op informatie berustende wilsuiting toestemming te verkrijgen van de gebruiker tot het plaatsen van cookies.[273]

Naar aanleiding van het Rapport voorlopige bevindingen van het CBP heeft TP Vision een toestemmingsvraag ingevoerd met een Ja/Nee-keuze voor het plaatsen en uitlezen van cookies om het kijkgedrag vast te kunnen leggen om daarmee persoonlijke kijkaanbevelingen te kunnen tonen (recommenderdienst) (zie p. 50-51 van dit rapport). Daardoor heeft TP Vision voldaan aan het criterium van een vrije wilsuiting.

Ten aanzien van de elementen 'specifiek' en 'geïnformeerd' in de zin van artikel 1, aanhef en onder i, van de Wbp heeft het CBP in paragraaf 3.5 van dit rapport vastgesteld dat TP Vision, ondanks een aantal maatregelen, betrokkenen (nog steeds) inconsistent en onvoldoende informeert over de verschillende gegevensverwerkingen.

TP Vision voldoet niet aan het criterium 'specifiek' omdat zij via de nieuwe toestemmingsvraag niet voor alle elementen van de gegevensverwerking toestemming vraagt. Uit de vraag en uit de onderliggende informatie valt niet op te maken welke gegevens precies voor welke doeleinden worden verwerkt. De termen 'regelmatig' en 'kijkgedrag' zijn onvoldoende specifiek, omdat daaruit niet af te leiden valt dat TP Vision elke drie tot vijf minuten cookies plaatst en uitleest, en dat onder 'kijkgedrag' ook het aan- en uitzetten van de tv, het kijken van *video on demand* en het gebruik van 'uitzending gemist'-apps is begrepen.

TP Vision voldoet evenmin aan het criterium 'geïnformeerd'. Zoals hierboven toegelicht (in paragraaf 3.5 van dit rapport) is de identiteit van de verantwoordelijke, TP Vision, onvoldoende kenbaar. De doeleinden van de gegevensverwerking zijn onvolledig, althans onvoldoende duidelijk omschreven in de NetTV Gebruiksvoorwaarden. Het CBP heeft vastgesteld dat als iemand de in deze gebruiksvoorwaarden genoemde URL in een browser invoert, hij belandt op een pagina die inmiddels buiten gebruik is en technische instellingsgegevens bevat van de webserver. De toestemmingsvraag met de daarbij gaande informatie die TP Vision

[273] Het CBP heeft bovenstaande toepassing van het toestemmingsvereiste in artikel 11.7a van de Tw voorgelegd aan de ACM in het kader van het Samenwerkingsprotocol CBP-OPTA van beide toezichthouders. De ACM stemt in met de voorgelegde toepassing van deze uitzonderingen in dit rapport.

heeft toegevoegd ten aanzien van het kijkgedrag is feitelijk onjuist als het gaat om de vindplaats van het privacybeleid (bij Philips). De informatie over de doeleinden van de gegevensverwerking is ook nog steeds niet vindbaar via zoekmachines.

Daar komt bij dat TP Vision tegenstrijdige informatie geeft over de verwerking en bewaartermijn van IP-adressen door IBM. TP Vision heeft daarover tegen het CBP verklaard dat IBM deze IP-adressen niet bewaart, maar is met haar bewerker IBM een feitelijk oneindige bewaartermijn overeengekomen (*stored permanently*) en vermeldt in haar Privacy Statement een bewaartermijn van maximaal 3 maanden.

Door het ontbreken van volledige en voldoende duidelijke informatie, kan van geïnformeerde toestemming geen sprake zijn.

TP Vision heeft (herhaaldelijk) aangegeven dat *tracking cookies* voor advertentiedoeleinden alleen met toestemming zullen worden geplaatst en uitgelezen. In haar zienswijze voegt TP Vision daaraan toe dat de advertentiecookies die nu al worden geplaatst, geen *tracking cookies* zijn. Ze worden ingezet "*ter voorkoming van het herhalen van advertenties op hetzelfde scherm, of, indien meerdere advertenties tegelijkertijd getoond kunnen worden, het gelijktijdig plaatsen van meerdere dezelfde advertenties op hetzelfde scherm*". TP Vision verstrekt daarbij alleen geaggregeerde en geanonimiseerde gegevens aan adverteerders over het aantal keren dat een advertentie is getoond, hoe lang de advertentie is bekeken en of er is doorgeklikt.

Uit het controle-onderzoek van het CBP van 3 juni 2013 blijkt dat TP Vision (nog steeds) géén toestemming vraagt aan betrokkenen voor het plaatsen en uitlezen van deze advertentiecookies.
TP Vision vraagt evenmin toestemming voor het plaatsen en uitlezen van gegevens van het toestel door IBM, waarmee informatie wordt verkregen over de door de gebruiker zelf ingevoerde URL's, bookmarks, appinstallatie, appgebruik en volgorde van de apps in het appscreen.

TP Vision vraagt ten slotte geen toestemming voor het plaatsen en uitlezen van analytische cookies door Google. De mededeling van TP Vision in haar Privacy Statement dat zij geen toestemming vraagt voor Google Analytics-cookies omdat dit geen persoonsgegevens zouden zijn, is onjuist. Er is wel degelijk sprake van een verwerking van persoonsgegevens, zoals vastgesteld in paragraaf 3.2 van dit rapport.

Bovendien ziet het toestemmingsvereiste uit de Tw op elke soort informatie die wordt geplaatst en uitgelezen op randapparatuur van gebruikers en niet alleen op persoonsgegevens.

Gerechtvaardigd belang

Het CBP heeft in paragraaf 2.2.2 (p. 27 e.v. van dit rapport) vastgesteld dat TP Vision cookies plaatst en uitleest om met adverteerders af te rekenen, om (met behulp van Google Analytics) gegevens te verzamelen over het gebruik van apps, en (met behulp van IBM) gegevens te verzamelen over het gebruik van apps en bezoek aan websites. TP Vision dient daarom voor deze drie soorten cookies te voldoen aan het bepaalde in artikel 11.7a van de Tw.

Het CBP heeft in de paragrafen 3.2 en 3.3 (p. 53 e.v. van dit rapport) vastgesteld dat hierbij eveneens sprake is van verwerking van persoonsgegevens. Omdat TP Vision deze cookiegegevens verzamelt in combinatie met het IP-adres en andere identificerende gegevens zoals het Consumer ID en Device ID van de smart tv-houder, zijn het in ieder geval voor TP Vision persoonsgegevens. TP Vision dient daarom ook een grondslag te hebben voor de gegevensverwerking als bedoeld in artikel 8 van de Wbp.

Het CBP heeft hierboven (p. 72 van dit rapport) vastgesteld dat TP Vision geen toestemming vraagt voor het plaatsen en uitlezen van de genoemde drie soorten cookies.

TP Vision heeft een (niet nader onderbouwd) beroep gedaan op de grondslagen van artikel 8, aanhef en onder b, c en f, van de Wbp voor de gegevensverwerkingen die resulteren uit het gebruik van de Philips smart tv.

Van een wettelijke verplichting (artikel 8, aanhef en onder c, van de Wbp) voor de gegevensverwerking zoals die thans door TP Vision plaatsvindt, is geen sprake. TP Vision is weliswaar gehouden mee te werken aan rechtsgeldige vorderingen om gegevens te verstrekken in het belang van de opsporing, maar dit betreft het beschikbaar stellen van aanwezige gegevens. Er is op dit punt geen verplichting tot het bewaren van gegevens.[274]

Voor zover TP Vision voor het gebruik van de (huidige) cookies die zij gebruikt om met adverteerders af te rekenen, voor de Google Analytics-cookies en de gegevens die IBM plaatst en uitleest een beroep zou willen doen op de grondslag van artikel 8, aanhef en onder b, van de Wbp, geldt het volgende.

Er is geen rechtvaardiging voor de verwerking aanwezig in de relatie tot (een overeenkomst met de) specifieke individuele betrokkene. TP Vision kan de overeenkomst met deze betrokkene goed uitvoeren zonder cookies te plaatsen en uit te lezen om met adverteerders af te rekenen en zonder (met behulp van Google Analytics en IBM) gegevens te verzamelen over het gebruik van apps respectievelijk het gebruik van apps en bezoek aan websites. Deze handelingen beogen meer het algemeen bedrijfsbelang van TP Vision te dienen, te weten: informatie verkrijgen om het gebruik van bepaalde apps en websites in kaart te brengen en te analyseren, zodat de kwaliteit van het Service Platform verbeterd kan worden.

Voor zover TP Vision voor het gebruik van de (huidige) cookies die zij gebruikt om met adverteerders af te rekenen, voor de Google Analytics-cookies en de gegevens die IBM plaatst en uitleest een beroep zou willen doen op de grondslag van artikel 8, aanhef en onder f, van de Wbp, geldt het volgende.

[274] De bewaarplicht verkeersgegevens is bijvoorbeeld niet van toepassing op diensten van de informatiemaatschappij, zoals TP Vision die levert.

Bij die rechtvaardigingsgrond dient het eigen gerechtvaardigde belang (bijvoorbeeld om zijn reguliere bedrijfsactiviteiten te kunnen verrichten) afgewogen te worden tegen de rechten en vrijheden van betrokkenen, in het bijzonder de bescherming van hun persoonlijke levenssfeer. Een verantwoordelijke die zich op deze grondslag wil beroepen, moet aantonen dat de verwerking noodzakelijk is: te weten de inbreuk op de belangen van de bij de verwerking betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel en dat het doeleinde is niet anderszins of met minder ingrijpende middelen te bereiken. Na deze afweging van proportionaliteit en subsidiariteit volgt een tweede afweging (privacytoets), waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. In het geval dat het belang van de betrokkene op bescherming van zijn persoonlijke levenssfeer doorslaggevend is, dient de verantwoordelijke af te zien van de gegevensverwerking.

Huidige advertentiecookies

Ten aanzien van het verzamelen en verwerken van gegevens over getoonde advertenties in combinatie met het Device ID en Consumer ID, ten behoeve van het doel om te kunnen afrekenen met adverteerders, zou in beginsel een beroep mogelijk zijn op artikel 8, onder f, van de Wbp (de noodzaak om deze gegevens te verzamelen ten bate van een gerechtvaardigd belang), mits TP Vision in voldoende waarborgen voorziet om te voorkomen dat het belang van betrokkenen bij de bescherming van hun persoonlijke levenssfeer prevaleert.

TP Vision heeft (in de huidige advertentiepilot) op zich een belangrijke waarborg getroffen jegens betrokkenen, door de gegevens zelf te verzamelen (zonder derde partijen in te schakelen) en geen (direct of indirect) identificerende gegevens te verstrekken aan de adverteerders. TP Vision verstrekt de adverteerders alleen geaggregeerde en geanonimiseerde gegevens over het aantal keren dat een advertentie is getoond en of dit tot resultaten heeft geleid. De gegevens die TP Vision aan de adverteerders verstrekt, zijn daarmee geen persoonsgegevens.

Omdat TP Vision ten aanzien van deze advertentiecookies echter niet voldoet aan artikel 11.7a van de Tw waaronder de verplichting om de gebruiker duidelijke en volledig te informeren overeenkomstig de Wbp en omdat TP Vision ook (met betrekking tot de privacytoets in artikel 8, onder f, van de Wbp) niet voorziet in een mogelijkheid voor betrokkenen om zich tegen de gegevensverwerking te verzetten, zijn er onvoldoende waarborgen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de betrokken smart tv houders. Transparantie is een noodzakelijke waarborg om ervoor te zorgen dat betrokkenen hun rechten kunnen effectueren, zoals het intrekken van toestemming. Hierdoor heeft TP Vision voor de verwerking van persoonsgegevens voor het doeleinde van afrekenen met adverteerders geen grondslag als bedoeld in artikel 8, aanhef en onder f, van de Wbp.

Ten overvloede merkt het CBP op dat indien het conceptwetsvoorstel tot aanpassing van artikel 11.7a Tw zoals dat in internetconsultatie is gegaan, wet wordt, beoordeling door het CBP op grond van de Wbp van de huidige werkwijze ten aanzien van deze soort cookies van TP Vision niet anders wordt. Dit vanwege het ontbreken van

aanvullende waarborgen door TP Vision als het gaat om de informatieverstrekking en het bieden van een reële en effectieve opt-outmogelijkheid.

Google analytics-cookies

Omdat TP Vision via de Google Analytics cookies gegevens verzamelt over individueel gebruik van verschillende apps, door de tijd heen, is sprake van zogenaamde *tracking cookies* waarmee (door Google of door TP Vision) profielen kunnen worden opgesteld.

Het gaat in dit specifieke geval dus om tracking van het appgebruik door individuele smart tv gebruikers, en niet om website analytics in zuivere vorm, dat wil zeggen, cookies waarmee het gebruik van één website wordt geregistreerd. Gegevens met betrekking tot appgebruik zijn, zoals eerder in dit rapport aangegeven, ook gegevens van gevoelige aard.

Om die reden komt alleen de grondslag ondubbelzinnige toestemming in aanmerking.

In haar opinie over cookies die vrijgesteld zijn van toestemming licht de Artikel 29-werkgroep toe dat analytics cookies niet voldoen aan de uitzonderingen op het toestemmingsvereiste voor het plaatsen en uitlezen van cookies, namelijk dat ze noodzakelijk zijn om de communicatie over een elektronisch communicatienetwerk uit te voeren, dan wel strikt noodzakelijk om een de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren. De werkgroep ziet evenwel geringe privacyrisico's in het gebruik van zogenoemde *first party* analytics cookies op voorwaarde dat ze strikt beperkt zijn tot deze *first party* (meestal een websitehouder), er voldoende informatie beschikbaar is en er ook anderszins waarborgen zijn getroffen die voorkomen dat de belangen van betrokkenen op bescherming van hun persoonlijke levenssfeer prevaleren.

De werkgroep schrijft: "*Such safeguards are expected to include a user friendly mechanism to opt-out from any data collection and comprehensive anonymization mechanisms that are applied to other collected identifiable information such as IP addresses.*"[275] De werkgroep vraagt de Europese Commissie dan ook bij een herziening van de e-Privacyrichtlijn een nieuwe uitzondering te creëren op het toestemmingsvereiste voor *first party* analytics cookies, mits "*strictly limited to first party anonymized and aggregated statistical purposes.*"

Hoewel TP Vision als waarborg heeft ingesteld dat Google het laatste octet van het IP-adres zo snel mogelijk na verzameling verwijdert, heeft TP Vision geen bewerkersovereenkomst gesloten met Google (waarin elke verdere verwerking voor eigen doeleinden van Google contractueel is uitgesloten). Het gaat bovendien juridisch niet om zogenaamde *first party* analytics cookies, maar om *third party* cookies.

[275] Artikel 29-werkgroep, Opinion 04/2012 on Cookie Consent Exemption (7 juni 2012) , p. 10. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Daar komt bij dat de verwerking (in ieder geval tot oktober 2012) intransparant was. De gebruikers werden niet geïnformeerd over het bestaan van deze gegevensverwerking en hadden en hebben geen reële en effectieve mogelijkheid om zich tegen deze gegevensverwerking te verzetten. De mogelijkheid om cookies te verwijderen uit de browser op het toestel bestaat alleen als een gebruiker de Gracenote-cookies heeft geaccepteerd om zijn kijkgedrag te registreren, en is dan alleen vindbaar via de Opties-knop op de afstandsbediening. Dat menu is alleen toegankelijk als de cursor in het aanbevelingsdeel van het scherm staat. Bovendien krijgen betrokkenen elke keer dat zij de tv aanzetten, via het Service Portal, automatisch nieuwe Google Analytics-cookies. TP Vision verstrekt in het Privacy Statement en de Cookie Policy weliswaar informatie over het gebruik van Google Analytics, maar stelt zich ten onrechte op het standpunt dat geen sprake is van persoonsgegevens.

Daargelaten dat de enige mogelijke grondslag voor dit specifieke gebruik van Google Analytics door TP Vision ondubbelzinnige toestemming is, kan TP Vision ook door het ontbreken van voldoende waarborgen (bewerkerscontract, informatie en een reële en effectieve opt-outmogelijkheid), ten aanzien van het (door Google laten) verzamelen en verwerken van gegevens over het gebruik van apps, in combinatie met het IP-adres, géén beroep doen op artikel 8, onder f, van de Wbp (de noodzaak om deze gegevens te verzamelen ten bate van een gerechtvaardigd belang).

IBM-cookies

Ook ten aanzien van het verzamelen en verwerken van gegevens (via IBM) over het gebruik van apps en bezoek aan websites (vier laatst bezochte URL's) is sprake van *tracking cookies* waarvoor op grond van de Wbp ondubbelzinnige toestemming is vereist. Het gaat hierbij om appgebruik en websitebezoek, door de tijd heen, waarmee (door TP Vision) profielen kunnen worden opgesteld. IBM bewaart het Consumer en Device ID en de IP-adressen in combinatie met de gegevens over het gebruik van apps en bezoek aan websites (de laatste vier bezochte URL's) voor onbeperkte tijd.

Om die reden komt alleen de grondslag ondubbelzinnige toestemming in aanmerking.

Hoewel TP Vision een bewerkersovereenkomst heeft gesloten met IBM[276], levert de verwerking toch privacyrisico's op voor betrokkenen, omdat het cookies betreft waarmee gebruik van verschillende apps en bezoek aan meerdere websites wordt vastgelegd *gedurende onbepaalde tijd*.

Omdat TP Vision niet transparant is (onvoldoende duidelijke informatie geeft) over de gegevensverwerking met behulp van de door IBM geplaatste cookies, geen andere waarborgen biedt zoals onmiddellijke anonimisering van de persoonsgegevens (Consumer ID, Device ID en IP-adressen), en niet voorziet in een reële en effectieve mogelijkheid voor betrokkenen om zich tegen deze verwerking te verzetten, weegt het

[276] Het CBP heeft bovenstaande toepassing van de begrippen 'first party cookies' en 'third party cookies' voorgelegd aan de ACM in het kader van het Samenwerkingsprotocol CBP-OPTA van beide toezichthouders. De ACM stemt in met de voorgelegde toepassing van deze begrippen in dit rapport.

gerechtvaardigd belang van TP Vision niet op tegen het belang van betrokkenen bij bescherming van hun persoonlijke levenssfeer.

Daargelaten dat de enige mogelijke grondslag voor dit specifieke gebruik van de IBM-cookies door TP Vision ondubbelzinnige toestemming is, heeft TP Vision hierdoor voor de verwerking van persoonsgegevens voor het doeleinde van het verzamelen van gegevens over gebruik van apps en bezoek aan websites (de vier laatst bezochte URL's) geen grondslag als bedoeld in artikel 8, aanhef en onder f, van de Wbp.

Omdat TP Vision ten aanzien van het plaatsen en lezen van geen van de drie genoemde soorten cookies ondubbelzinnige toestemming krijgt van betrokkenen, en geen beroep kan doen op een andere grondslag in artikel 8 van de Wbp, handelt TP Vision ten aanzien van de verwerking van persoonsgegevens in het geval van alle drie de besproken soorten cookies in strijd met het bepaalde in artikel 8 van de Wbp, jo. 11.7a van de Tw.

CONCLUSIES

TP Vision bepaalt sinds 1 april 2012 doel en middelen voor het verzamelen en verwerken van gegevens over Nederlandse gebruikers van de Philips smart tv. TP Vision is daarmee verantwoordelijk voor de gegevensverwerkingen via de Philips smart tv.

Het CBP constateert dat TP Vision het onlinekijkgedrag, gebruik van apps en websitebezoek (op hoofddomein) van de gebruikers van Philips smart tv's door middel van cookies verzamelt en deze persoonsgegevens bewaart. Ook verzamelt en bewaart TP Vision per smart tv wanneer er tv wordt gekeken, welke uitzendingen en apps favoriet zijn, welke uitzendingen een gebruiker opneemt, welke video's een gebruiker huurt en welke 'uitzending gemist'-uitzendingen een betrokkene bekijkt. Dit zijn 'gevoelige' persoonsgegevens. De gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek etc. kunnen een indringend beeld kunnen geven van iemands communicatiegedrag en soms ook iets zeggen over de inhoud van de communicatie.

TP Vision is in staat om betrokkenen gericht te benaderen, bijvoorbeeld via de 'recommenderdienst' die programma's aanbeveelt op grond van profielen van historisch onlinekijkgedrag, kan consumentenprofielen opstellen en kan betrokkenen benaderen per e-mail en per sms.

Overtredingen die nog niet zijn beëindigd

Informatieplicht
TP Vision is wettelijk verplicht gebruikers te informeren over de verwerking van hun persoonsgegevens. Zij moeten namelijk zicht (kunnen) hebben op het aantal en de soort verwerkingen die plaatsvinden met hun persoonsgegevens en de gevolgen daarvan, ook op de lange termijn.

TP Vision geeft gebruikers in Nederland onvolledige en onvoldoende duidelijke informatie over haar identiteit en over de gegevensverwerking via de Philips smart tv's. Voor een gebruiker van een Philips smart tv was (en is) het onvoldoende inzichtelijk wie TP Vision is, welke cookies er worden geplaatst en uitgelezen door TP Vision en haar bewerkers, welke persoonsgegevens er worden verzameld en hoe lang deze persoonsgegevens worden bewaard. Ondanks herstelmaatregelen is TP Vision hierdoor (nog) in overtreding. De informatie in de gebruiksvoorwaarden, het Privacy Statement en de Cookie Policy was (en is) onvoldoende publiek toegankelijk en inconsistent. Hierdoor handelt TP Vision in strijd met artikel 34 van de Wbp (de plicht om betrokkenen te informeren als de persoonsgegevens niet rechtstreeks worden verkregen).

Daarnaast is onvoldoende duidelijk dat registratie van klantgegevens (bij Philips) optioneel is. Hierdoor handelt TP Vision in strijd met artikel 33 van de Wbp (de plicht om betrokkenen te informeren als de persoonsgegevens van henzelf worden verkregen).

Cookies en toestemming
TP Vision plaatst gegevens op en leest informatie uit van Philips smart tv's, deels met behulp van cookies. Omdat het geen technisch noodzakelijke (zogeheten 'functionele') cookies betreft die uitgezonderd zijn van het toestemmingsvereiste uit de Telecommunicatiewet (Tw), moet TP Vision hiervoor geïnformeerde toestemming vragen en verkrijgen.

Hierbij vindt tegelijkertijd ook een verwerking van persoonsgegeven plaats. Voor die verwerking moet een wettelijke rechtvaardigingsgrond (grondslag) bestaan. Ten aanzien van de cookies waarmee TP Vision het kijkgedrag vastlegt, is de enige rechtsgeldige grondslag ondubbelzinnige toestemming.

Wil er sprake zijn van rechtsgeldige toestemming, dan dient er sprake te zijn van een vrije, specifieke en op informatie berustende wilsuiting (artikel 1, onder i, van de Wbp) waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

TP Vision heeft op 18 april 2013 (voor nieuwe gebruikers), respectievelijk 2 juni 2013 (voor bestaande gebruikers), een toestemmingsvraag ingevoerd voor cookies die het kijkgedrag vastleggen, om persoonlijke kijkaanbevelingen te kunnen tonen. Door het ontbreken van volledige en duidelijke informatie voldoet de toestemming niet aan de criteria 'specifiek' en 'op informatie berustend'. Voor de advertentiecookies en de analytische cookies waarmee het appgebruik wordt vastgelegd, respectievelijk appgebruik én websitebezoek, vraagt TP Vision in het geheel geen toestemming. Omdat TP Vision geen ondubbelzinnige toestemming en ook geen andere grondslag heeft voor deze verwerkingen, handelt TP Vision in strijd met het bepaalde in artikel 8 van de Wbp, jo. 11.7a van de Tw.

Bewerkerscontract
Op grond van de Wbp is een bedrijf verplicht een bewerkersovereenkomst te sluiten als een ander ten behoeve van het bedrijf persoonsgegevens verwerkt. TP Vision handelt in strijd met artikel 14 van de Wbp omdat zij geen bewerkersovereenkomst heeft gesloten met Google voor het verwerken van persoonsgegevens door Google Analytics.

Google heeft schriftelijk geweigerd een dergelijke overeenkomst aan te gaan. TP Vision heeft toegezegd de overtreding te zullen beëindigen door later dit jaar over te gaan op een eigen *analytics*-systeem.

Getroffen maatregelen en overtredingen die daardoor (gedeeltelijk) zijn beëindigd

Bewerkerscontracten
TP Vision maakt gebruik van de diensten van andere bedrijven voor de levering van de onlinediensten. Vier van deze bedrijven verwerken ten behoeve van TP Vision persoonsgegevens van de gebruikers van de smart tv's. Naar aanleiding van het onderzoek heeft TP Vision bewerkerscontracten gesloten met Gracenote, IBM en MPP Global (en indirect met Akamai). Door deze getroffen maatregel zijn de geconstateerde overtredingen van artikel 14 van de Wbp op dit punt beëindigd.

Informatieplicht
Vanaf medio oktober 2012 heeft TP Vision een deel van de geconstateerde overtredingen met betrekking tot de informatieverstrekking verholpen. TP Vision heeft de gebruiksvoorwaarden uitgebreid met een Privacy Statement en een Cookie Policy. TP Vision heeft bovendien de gegevensverwerking gemeld bij het CBP. TP Vision heeft na ontvangst van het Rapport voorlopige bevindingen van het CBP informatie over de bewaartermijnen van de persoonsgegevens toegevoegd aan een nieuwe versie van het Privacy Statement en de Cookie Policy (per 1 mei 2013). Door deze getroffen maatregelen is de overtreding van de informatieplicht deels beëindigd.

Bijlage I Print-out TP Vision privacy statement van 12 oktober 2012

SMART TV PRIVACY STATEMENT

Date: October 12th 2012

IN THIS PRIVACY STATEMENT WE DESCRIBE HOW WE COLLECT, STORE OR OTHERWISE PROCESS PERSONAL DATA IN RELATION TO YOUR USE OF THE SMART TV PORTAL AND FOR WHICH SPECIFIC AND LEGITIMATE PURPOSES SUCH PROCESSING TAKES PLACE. IN ADDITION TO THIS PRIVACY STATEMENT WE ALSO HAVE A COOKIE POLICY, WHICH IS ACCESSIBLE HERE. WE ARE TP VISION NETHERLANDS B.V. WITH OFFICES AT PRINS BERNHARDPLEIN 200 (1097 JB) AMSTERDAM THE NETHERLANDS. WE ARE A 100% SUBSIDIARY OF TP VISION HOLDING B.V. TP VISION HOLDING B.V. IS A JOINT VENTURE BETWEEN TPV TECHNOLOGY LIMITED AND KONINKLIJKE PHILIPS ELECTRONICS N.V.

PLEASE REGARD US AS BEING THE DATA CONTROLLER FOR YOUR PERSONAL DATA. WE USE VARIOUS OUTSOURCING PARTNERS TO PROCESS PERSONAL DATA ON OUR BEHALF, SOME OF WHICH ARE DATA PROCESSORS FOR YOUR PERSONAL DATA.

"APP" means an application that is displayed in the Portal by means of a branded Icon, which provides access to a Content Partner website.

"Content Partner Website" means a website offered by a third party that is accessible through a hyperlink on the Portal, through which you can obtain access to his content.

"Consumer ID" means a unique number to identify a consumer on the Platform.

"Club Philips" means a customer loyalty program operated by Philips.

"Device" means any Internet connected product, which is capable to access the Portal and has been certified by us.

"Device Manufacturer" means the third party that has manufactured a Device.

"Device Portal" a Device authentication server, used to authenticate and identify Devices.

"IP-EPG" means the Electronic Program Guide provided by us, which is accessible by pushing the "Guide" button on the remote control of the Device, or by means of the menu on the Device. The IP-EPG is available on select Devices in select countries and TV networks.

"Mobile Device" means an iPad or other mobile Internet connected product.

"Personal Data" means any information relating to an identified or identifiable natural person, like a name, e-mail address or IP number.

"Philips" means Koninklijke Philips Electronics N.V. and/or its subsidiaries.

"Platform" means the technical IT infrastructure that is used by us to manage and operate the Portal and the services we provide via the Portal, which includes (web)servers, databases and related network infrastructure.

"Portal" means our SmartTV Portal.

"Processing of personal data" means any operation or set of operations which is performed by us or on our behalf, upon personal data, whether or not by automatic means, such as, but not limited to collection, storage, transmission and adaptation.

"URL" means uniform resource locator. This is the web address of a site, which is inserted in the navigation bar of the browser of your Device.

"You" means the natural person whose personal data is collected and processed by us.

Below we will first describe which data is collected in relation to your Device. We will then tell you how we process this data and for which purposes. At the end of this privacy statement we will describe how we keep your data secure, whether data is transmitted outside of the European Union and how you can utilize your statutory rights to have us change or delete personal data. Please note that we are not responsible for all of the processing of data described below. Because this processing is connected with your use of a Device

however, we have included a description of it in our privacy statement.

-

Which types of data are collected?

Identification numbers

Consumer-ID: For each Device that is authenticated on a Device Portal, that Device Portal will generate and store a unique number to enable it to distinguish between different Device owners. This is the Consumer-ID. As explained below, the Consumer-ID may be linked to personal data provided by you during registration with Club Philips or a customer loyalty program or warranty registration from a Device Manufacturer. If you do not register for such program or for warranty purposes, the Consumer-ID is anonymous. Depending on your Device, Philips or the Device Manufacturer, which manufactured your Device, is the data controller for the Consumer-ID. We receive the Consumer-ID without the corresponding registration data. As a consequence the Consumer-ID does not constitute personal data for us.

Device-ID: For each Device that is authenticated on a Device Portal, that Device Portal will generate and store a fixed unique number to enable us to authenticate and identify the Device on the Platform. This number is called the Device-ID. We provide the Device-ID to selected content partners for authentication purposes. These content partners use the Device-ID to authenticate your Device for access to a Content Partner Website, provide us with viewing data for Video on Demand Titles and offer promotions and discounts. If you use a Mobile Device to utilize part of the functionality of the Portal, for example by using our "MyRemote APP", we will assign such use to the Device-ID of the Device.

Mobile Device-ID: If you use a Mobile Device to utilize a part of the functionality of the Portal, we will store a unique identifier for that Mobile Device.

Data collected during initialization

Registration: When you initialize your Device you may be given the option to register your Philips Device with Club Philips. For other Devices you may be given the option to register your Device with a customer loyalty program from the Device Manufacturer or register your Device for warranty purposes with the Device Manufacturer. As part of this registration you will need to provide personal data, such as your name, e-mail address, country of residence and specific details about your Device like type and serial number. Registration is not obligatory, if you don't like to register you can skip this registration, this will not affect your use or your statutory warranty on the Device. We don't receive nor do we process any of the data relating to your registration. The Device Portal does transmit to us whether you have registered or not, and whether you have accepted the Portal terms and conditions. This information is linked to the Consumer-ID.

Portal sign-on data: Whenever you connect your Device to the Internet, it will automatically connect to its Device Portal. The Device Portal will authenticate your Device as being certified for access to the Portal. For authentication purposes, the Device Portal contains one or more unique numeric identifiers related to your Device. Upon authentication your Device receives a Device-ID and will be redirected to the Portal. The Device Portal is managed by one of our outsourcing partners. If you don't have a Philips Device the Device Portal can also be managed by the Device Manufacturer or by an outsourcing partner of the Device Manufacturer.

APP placement: As part of the regular functionality of the Portal you can manually arrange the order in which APPs are displayed on your home screen in the Portal. We will store your initial arrangement and any changes you make afterwards, linked to the Consumer-ID and the Device-ID.

Device specific information: When you first log on to the Portal, the Device-ID is linked to a record of specific Device related information. This information includes the Device type, and the language and country that have been configured in the Device.

Data collected during use

Advertising: In-video and display advertisements (banners) are served within the Portal, the IP-EPG, and within content that is accessible by means of Content Partner Websites. These advertisements are served by us, or by third parties using advertising inventory assigned by us. All advertisements are served by means of our advertising server. Our advertising server or the third party advertising server will set a cookie on your Device. By means of the cookie we can monitor which advertisements were shown to you Device and whether someone using the Device has clicked on an advertisement. We will not set a cookie on your Device without your permission.

Portal and Content Partner Website traffic, browser history and APP click behavior: When you use the Portal you will generate direct Internet traffic between your Device and the Portal and Content Partner Websites that are accessible through the Portal. As part of this traffic we receive the IP address of your Internet connection and the language and country that has been configured in your Device. This information is stored in a on the Platform. We also store IP addresses within the database of the IP-EPG. server log.

Each URL that is inserted by you in the navigation bar of the browser of your Device is stored on the Platform and linked to the Consumer-ID and the Device-ID. When you click on an APP we will only store this click and the date and time on which you performed the click. Your APP clicks are stored in a database record, linked to the Consumer-ID and the Device-ID.

For data that is linked to the Consumer-ID and the Device-ID, you have the option to unlink it from those identifiers by means of the "Clear Net TV Memory" or "Reinstall Device" option in the menu on your Device. After unlinking this data will remain stored for aggregate statistics, but will not be linked anymore to the Consumer-ID or the Device-ID. This option not only deletes all cookies and local browser storage, it also unregisters your Device from any registrations. On newer Devices, this option is called "Reinstall Device". These newer Devices also have an option "Clear App Memory", which only deletes all cookies and local browser storage, but does not unregister your Device. It is highly advisable to always "Clear Net TV Memory" or "Reinstall Device" prior to selling your Device or giving it away.

We use Google Analytics to store and monitor your interaction with the Portal by means of your Device or Mobile Device. This data is not linked to the Consumer-ID or the Device-ID, and it is stored in an anonymous fashion because we have configured. Google Analytics to apply IP address anonymization. The IP anonymization feature in Google Analytics removes the last octet of IPv4 visitor IP addresses and the last 80 bits of IPv6 addresses in memory shortly after being sent to the Google Analytics Collection Network. The full IP address is never written to disk.

The Portal is managed by one of our outsourcing partners.

When you visit a Content Partner Website, the content partner in question will receive the IP address of your Internet connection and the language and country configured in your Device. We do not store or otherwise process actual Internet traffic between your Device and a Content Partner Website, nor can we view this traffic. The content partner is the data controller for any personal data he receives by means of a Content Partner Website.

Zap behavior: If you have activated personalized recommendations, we will periodically store zap behavior. By zap behavior we mean which television programs were watched on or via your Device and how users of your Device change between television channels. Generally we store the currently watched channel periodically in a cookie on your Device. When this cookie is refreshed we receive a copy of the data stored in this cookie. This data is then stored within the recommendation engine of the Portal. The recommendation engine is a part of the Platform and is responsible for providing Device specific viewing recommendations in the Portal and in the IP-EPG. . If you use a Mobile Device to access the functionality of the IP-EPG we will also store the system name of the Mobile Device (for example "Tom's iPad"). The recommendation engine is managed by one of our outsourcing partners.

Rented Video on Demand titles: Each content partner provides us with an overview of the rented Video on Demand titles per Device-ID. This overview is subsequently stored within the recommendation engine.

Catch-Up TV APP viewing data: Our Catch-Up TV APP, available for selected countries, enables you to watch regular television programs, which have already been broadcasted. When this APP is used we will store the television programs that have been watched. This information is linked to the Device-ID.

Data collected as part of SmartTV payment transactions: In the Portal we provide for the possibility of opening a SmartTV payment account. When you open an account you will be requested to provide your name, country of residence, e-mail address and information related to the payment instrument you wish to utilize (credit card, bank debit etc). For security purposes we will link your payment account to the Device-ID of your Device. Any data that we store in relation to a SmartTV payment account is processed by our payment service provider in accordance with all applicable security standards, as we will further explain below.

What do we do with the data we collect?

We process collected data for the following purposes:

- **Maintaining and operating the Portal**: We use the IP address, Consumer-ID, Device-ID, and the country and language configured on your Device, to be able to provide your Device with access to the Portal and Content Partner Websites, and provide it with the correct APP view. This includes but is not limited to use for the purposes of authentication, abuse handling, management of security incidents, monitoring of availability of the Portal and Content Partner Websites, and providing backup services of user preferences.
- **Optimizing the user experience of the Portal**: We use aggregate and anonymized usage data like APP click behavior, APP preferences, browser history and your interaction with the Portal to improve and further develop the Portal user experience.
- **Payment Transactions**: We use the information in your SmartTV payment account to process and authorize your payment transactions.
- **Improve open Internet browsing**: We use your browser history to enable us to generate thumbnails for URLs which were inserted in the navigation window of the browser of the Device and to enable an autocomplete function for these URLs.
- **Optimizing advertisement experience:** We use data related to advertising views and clicks on advertisements to optimize the advertising experience of consumers in the Portal.
- **Device specific viewing recommendations:** Provided you have activated personalized viewing recommendations in the Portal, we use the zap behavior, rented Video on Demand titles, Catch-Up TV and APP viewing data related to your Device-ID, to generate Device specific recommendations for viewing television programs and Video on Demand in the recommendations section of the Portal and the IP-EPG.
- **Discounts:** we provide the Device-ID to selected content partners to enable these partners to identify to what extent they can provide you with free access to Video on Demand titles in their collection.
- **Authentication:** We provide the Device-ID to selected Content Partners for authentication purposes.
- **Law enforcement:** We may be required to provide data to competent law enforcement officials or judicial authorities. If we do so it will always be subject to a binding legal instrument like a warrant or a judicial order or other rule of applicable statutory law, which would require us to cooperate with law enforcement or judicial authorities.

Is data transmitted outside of the European Union?

All personal data that is processed by us and by our outsourcing partners is stored and processed on servers that are based in the European Union. We do utilize the AKAMAI content distribution system to ensure that content relating to the Portal is cached nearby the geographic location of your Device, to improve speed and user experience. AKAMAI servers are also outside of the European Union. Content distribution and dissemination via AKAMAI is initiated on the basis of your use of content that is accessible by means of the Portal. If a number of Devices request the same content, the AKAMAI system will automatically cache such content on a node that is geographically near to these Devices, i.e. if multiple TVs in Russia request content, content may be cached on an AKAMAI node that is located in Russia. For more information on AKAMAI please visit: http://www.akamai.com.

How secure is your personal data?

The connection between your Device and the Device Portal is encrypted. The state of this encryption has been audited by a reputable firm of auditors and has been confirmed to be suitably secure.

All Internet traffic between your Device, the Portal and the IP-EPG, is secured by SSL (secured socket layer), or an equivalent encryption technology. Whether or not a connection between your Device and a Content Partner Website is encrypted depends on the settings on the Content Partner Website. When your Device is connected to a Content Partner Website, you can check the encryption status of the connection in the Portal. Please check the manual of your Device.

Your stored personal data is maintained in a secure environment, which is regularly audited in accordance with accredited audit standards. Access to this data is password protected and role based, i.e. limited to our employees and those of our outsourcing partners

who need to access it as part of their job description.

Credit card information you provide to us is stored in accordance with the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS Tier 1). If you would like to know more about PCI-DSS, please visit: https://www.pcisecuritystandards.org/.

Contacting us

You can send us an e-mail via privacy@tpvision.com in your own language. You can use this e-mail address if you have any questions regarding our privacy policy, would like to request a copy of your personal data or if you want us to change or delete your personal data.