

College bescherming persoonsgegevens

Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door KPN B.V.

Z2011-00462

Rapport definitieve bevindingen
Mei 2013 met corrigendum van 12 juni 2013

OPENBARE VERSIE

Inhoudsopgave

Samenvatting	3
1. Inleiding.....	6
2. Feitelijke bevindingen.....	15
2.1 Organisatiebeschrijving	15
2.2 Mobiel netwerk, netwerkverkeer en plaatsing data-analyse apparatuur.....	17
2.3 Overzicht doeleinden.....	20
2.4 Netwerkplanning en -beheer	21
2.5 Prepaid- en MMS-verkeer	34
2.6 Firewalls, spamfilters en virusscanners.....	38
2.7 Behandeling van klantklachten	41
2.8 Verdere verwerking	43
3. Uitwerking van het wettelijk kader en beoordeling	47
3.1 Wettelijk kader: samenloop Wbp en Tw	47
3.2 Verantwoordelijke	49
3.3 Verwerking van persoonsgegevens.....	49
3.4 Verkeersgegevens versus communicatie.....	58
3.5 Gegevensverwerking	63
3.6 Grondslag	64
3.6.1 Netwerkplanning en -beheer	76
3.6.2 Prepaidverkeer.....	81
3.6.3 Firewalls, spamfilters en virusscanners.....	83
3.6.4 Behandeling van klantklachten	85
3.6.5 Verdere verwerking.....	87
3.7 Uitdrukkelijk omschreven en gerechtvaardigde doeleinden.....	89
3.8 Informatieplicht	91
3.9 Meldingsplicht	95
3.10 Behoorlijk en zorgvuldig verwerken van persoonsgegevens	97
4. Conclusies.....	98

Bijlagen:

- I. Schema mobiel netwerk
- II. Standaardlijst bijgehouden applicaties en websites [VERTROUWELIJK: apparatuur]
- III. Overzicht verwerkte gegevens, per doeleinde
- IV. Verklarende woordenlijst
- V. Zienswijze 1 KPN, met de reactie daarop van het CBP
- VI. Zienswijze 2 KPN, met de reactie daarop van het CBP

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar de wijze waarop KPN *packet inspection* technologie en technieken (hierna: data-analyse technieken) toepast in het mobiele netwerk van het bedrijf. Onder data-analyse technieken wordt verstaan: technieken waarmee gegevens over en uit het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd. Het CBP heeft onderzocht of KPN hierbij persoonsgegevens verwerkt en zo ja, of KPN zich houdt aan de Wet bescherming persoonsgegevens (Wbp) en hoofdstuk 11 van de Telecommunicatiewet (hierna: Tw).

Achtergrond onderzoek

Een belangrijke reden voor veel telecombedrijven om data-analysetechnieken in te zetten is netwerkbeheer, om te zorgen dat het mobiele netwerk goed functioneert en niet overbelast raakt. Daarnaast gebruiken bedrijven de technieken voor andere doeleinden, zoals facturering, marktonderzoek, blokkering van bepaalde internettoepassingen, spam- en virusfiltering en klachtafhandeling.

Het gebruik van data-analyse technieken - en een eventuele privacyschending hierbij - raakt veel mensen. Eind 2012 waren er ruim 22 miljoen mobiele telefonieaansluitingen in Nederland, waarvan 10,2 miljoen met mobiel internet.

Data-analyse bij KPN

KPN verwerkt gegevens over en uit het dataverkeer van circa 4 miljoen KPN abonnees met mobiel internet. Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn. Het gaat onder meer om gegevens over welke websites iemand bezoekt en de apps die deze persoon gebruikt.

KPN verwerkt de persoonsgegevens voor vier doeleinden:

- netwerkplanning en -beheer;
- het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed (hierna 'prepaidverkeer' genoemd);
- het gebruik van firewalls, spamfilters en virusscanners (hierna 'spam- en virusfiltering' genoemd); en
- de behandeling van klantklachten (het oplossen van technische incidenten en klantproblemen in individuele gevallen).

KPN inspecteert en analyseert meestal alleen gegevens over het dataverkeer, niet de inhoud ervan. De gegevens over het dataverkeer kunnen evenwel toch inhoudskenmerken bevatten, zoals informatie over bezochte websites en gebruikte apps. Dat soort gegevens zijn 'gevoelige' persoonsgegevens. Enkel gedownloade bestanden en verzonden en ontvangen e-mails inspecteert en analyseert KPN ook op inhoud teneinde spam, virussen en malware tegen te houden en te verwijderen.

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Eén van die eisen is dat er een rechtvaardigingsgrond (grondslag) moet zijn voor de verwerking. Het CBP heeft bij KPN gedurende het onderzoek een aantal overtredingen van de Wbp én de Tw geconstateerd die inmiddels zijn beëindigd.

Netwerkplanning en -beheer

Het verwerken van persoonsgegevens voor het doeleinde netwerkplanning en -beheer is alleen toegestaan als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren. Omdat KPN de persoonsgegevens niet zo snel mogelijk verwijderde, was het bedrijf in overtreding.

Prepaidverkeer

Om prepaid abonnees in staat te stellen opwaardeersites te bezoeken als hun tegoed op is, verwerkte KPN URL's om de gratis opwaardeersites te herkennen. KPN verwerkte voor dit doeleinde persoonsgegevens van méér abonnees dan alleen degenen met een ontoereikend prepaid tegoed, terwijl er ook andere mogelijkheden waren. Omdat deze gegevensverwerking onevenredig is, was KPN hierdoor in overtreding.

Spam- en virusfiltering en klachtbehandeling

KPN heeft wel een wettelijke grondslag voor de verwerking ten behoeve van spam- en virusfiltering en klachtbehandeling. Op deze punten is KPN dan ook niet in overtreding (geweest).

Informeren abonnees

KPN is wettelijk verplicht abonnees 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. KPN informeerde abonnees niet over de gegevensverwerking bij de toepassing van data-analyse technieken voor de doeleinden netwerkplanning en -beheer en prepaidverkeer. Daarnaast informeerde KPN hen niet over de categorieën van verwerkte persoonsgegevens en de bewaartermijn. KPN was hierdoor in overtreding.

Meldingsplicht

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen wettelijk verplicht deze gegevensverwerking te melden bij het CBP. De meldingen van KPN waren niet volledig en niet duidelijk genoeg over het verwerken van persoonsgegevens ten behoeve van prepaidverkeer en spam- en virusfiltering. KPN was hierdoor in overtreding.

WhatsApp

Het is niet behoorlijk en niet zorgvuldig en dus in strijd met de wet dat KPN eenmalig (over de periode februari-april 2011) op abonneeniveau gegevens heeft verstrekt over het WhatsApp-gebruik aan het KPN retailbedrijf voor marktonderzoek (analyse van de eigen dienstverlening). KPN is hierdoor in overtreding geweest.

Getroffen maatregelen

Naar aanleiding van het onderzoek heeft KPN de meldingen bij het CBP en de privacyverklaringen van het bedrijf aangepast.

KPN heeft besloten de data-analysetools voor netwerkplanning en -beheer en prepaidverkeer stop te zetten met ingang van 21 september 2012 respectievelijk 3 oktober 2012.

KPN heeft de voor netwerkplanning en -beheer opgeslagen gegevens én de geanonimiseerde gegevens die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening verwijderd.

Door deze getroffen maatregelen zijn de geconstateerde overtredingen beëindigd.

KPN heeft de data-analysetool voor netwerkplanning en -beheer aan laten passen zodat gegevens zo snel mogelijk na het verzamelen worden geanonimiseerd. KPN verwacht de nieuwe versie van de software per 1 juni 2013 in gebruik te nemen.

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 KPN B.V. (hierna: KPN) in haar mobiele netwerk *packet inspection* technologie en technieken (hierna: data-analyse technieken) toepast.

Het CBP heeft onderzocht of KPN hierbij persoonsgegevens verwerkt en zo ja, of KPN zich houdt aan de Wbp en hoofdstuk 11 van de Telecommunicatiewet (hierna: Tw).

Onder data-analyse technieken wordt hier verstaan: het gebruik maken van technieken waarmee gegevens *over* en *uit* het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd.

Achtergrond onderzoek

Mobiele netwerken bestaan vandaag de dag vaak uit een GSM-gedeelte (voor de afhandeling van spraakverkeer) en een GPRS/UMTS-gedeelte (voor de afhandeling van dataverkeer).¹ Deze gedeeltes staan in verbinding met elkaar. Mobiele apparaten, zoals smartphones, gebruiken beide gedeeltes van het netwerk, al naar gelang de gebruikte dienst (spraak of data).

Mobiele netwerken vervoeren niet alleen spraak- en dataverkeer, maar ook signaleringsverkeer (kleine berichten die nodig zijn om de verbinding op te bouwen, in stand te houden en te verbreken).² Spraak-, data- en signaleringsverkeer maken gebruik van dezelfde radioweg (toegang tot het mobiele netwerk). Elk onderdeel van het mobiele netwerk heeft een maximum capaciteit.

Er zijn applicaties (*apps*) die voortdurend dataverkeer uitwisselen met de dichtstbijzijnde zendmasten, ook zonder dat een abonnee dat merkt, om de verbinding met het internet 'open' te houden. Dit fenomeen wordt wel 'chatty apps' genoemd en leidt tot een significante toename van het signaleringsverkeer. Als het radiotoegangsnetwerk crasht als gevolg van teveel signaleringen in het GPRS/UMTS-gedeelte kan er ook niet meer worden gebeld.

Een belangrijke aanleiding voor veel mobiele netwerkaanbieders om data-analyse technieken in te zetten is netwerkbeheer, om te voorkomen dat op momenten van veel dataverkeer en/of signaleringen in het GPRS/UMTS-gedeelte (het spraakgedeelte van) het netwerk overbelast raakt.³

¹ Mobiele netwerken zijn daarnaast verder te verdelen in een radiotoegangsnetwerk- en een *core*-netwerkgedeelte (vgl. **bijlage I**).

² Een signalering kan bijvoorbeeld de volgende categorieën van gegevens bevatten: het 06-nummer (*Mobile Subscriber ISDN Number*; MSISDN), het unieke klantnummer (*International Mobile Subscriber Identity*; IMSI), het unieke toestelnummer (*International Mobile Equipment Identity*; IMEI), zendmastgegevens (*Cell ID*), de starttijd en eindtijd van de data sessie etc.

³ Zie o.a. 'Smartphones overbelasten netwerk T-Mobile', *AutomatiseringGids* 31 mei 2010, over de overbelasting van het T-Mobile netwerk door dataverkeer van smartphones en met name de nieuw geïntroduceerde iPhone medio 2010. Iets soortgelijks gebeurde met het AT&T netwerk in de Verenigde Staten. URL:

Data-analyse technieken worden in de huidige praktijk niet alleen ingezet voor technisch netwerkbeheer, maar ook voor andere doeleinden, zoals facturering (waaronder het afzonderlijk in rekening brengen van bepaalde protocollen en diensten), het blokkeren van bepaalde protocollen en diensten, spam- en virusfiltering, afhandeling van klantklachten en marketing.

Het gebruik van data-analyse technieken raakt veel mensen. Volgens gegevens uit de jaarlijkse marktmonitor van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: OPTA, per 1 april 2013 Autoriteit Consument en Markt, hierna: ACM) waren er aan het einde van het derde kwartaal van 2011 21,8 miljoen mobiele aansluitingen in Nederland, waarvan 8,2 miljoen met een (prepaid of postpaid) data abonnement,⁴ en aan het einde van het vierde kwartaal van 2012 22 miljoen mobiele aansluitingen, waarvan 10,25 miljoen met een data abonnement.⁵ Vodafone en T-Mobile hebben de meeste smartphone abonnees, waarna KPN volgt op enige afstand.⁶ Tele2 volgt op zeer grote afstand, met een marktaandeel van bijna 2,5% van de mobiele telefonieaansluitingen met een data abonnement.⁷

<http://www.automatiseringgids.nl/nieuws/2010/22/smartphones-overbelasten-netwerk-t-mobile> (URL laatst bezocht op 29 mei 2013).

⁴ 'OPTA jaarverslag en marktmonitor 2011', Mededeling OPTA 23 april 2012. URL: <https://www.acm.nl/nl/publicaties/publicatie/10347/OPTA-jaarverslag-en-marktmonitor-2011/>. Presentatie marktmonitor 2011. URL: <https://www.acm.nl/nl/publicaties/publicatie/10346/Presentatie-marktmonitor-2011/> (URL laatst bezocht op 29 mei 2013).

⁵ "Het totaal aantal aansluitingen met mobiel breedband is eind 2012 ruim 10 miljoen: 9,1 miljoen mobiele telefoons en 1,2 miljoen tablets en dongels." ACM Nieuwsbericht Telecommonitor 2012, Lagere omzet voor mobiele aanbieders door minder sms'jes', 17 april 2013, URL: <https://www.acm.nl/nl/publicaties/publicatie/11338/Telecommonitor-2012-Lagere-omzet-voor-mobiele-aanbieders-door-minder-smsjes/> (URL laatst bezocht op 29 mei 2013).

⁶ Van de totaal 22.098.000 mobiele aansluitingen aan het eind van 2012 in Nederland, waren er 9.063.000 met mobiel breedbandinternet en 1.185 specifieke mobiele breedbandaansluitingen, zoals tablets en dongels. In totaal 10.248.000 mobiele internetaansluitingen, ofwel 46,4 procent van het totaal aantal mobiele aansluitingen. Bron tabel "Mobiel: Marktaandelen retail aansluitingen" uit de ACM Openbare rapportage mobiel Q4, p. 1, URL: <https://www.acm.nl/nl/download/bijlage/?id=10942> (URL laatst bezocht op 29 mei 2013). Het feitelijke percentage mobiele aansluitingen met data-abonnement verschilt per operator. Vgl. 'Consumenten kopen handset in winkel, bestellen sim online', *Telecompaper* 11 juli 2012. URL:

<http://www.telecompaper.com/nieuws/consumenten-kopen-handset-in-winkel-bestellen-sim-online> (URL laatst bezocht op 29 mei 2013). Vgl. ook TNO Marktrapportage Elektronische Communicatie (MEC) eerste helft 2012, 18 februari 2013, URL: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2013-02-18%2016:42:09.0 (URL laatst bezocht op 29 mei 2013).

⁷ Eind eerste kwartaal 2013 had Tele2 535.000 mobiele abonnees in Nederland. Bron: financiële kwartaalreportage Tele2 Q1 2013, URL: <http://reports.tele2.com/2013/Q1/index.html> (URL laatst bezocht op 29 mei 2013). Omgerekend vanuit het gegeven dat gemiddeld 46,4% van de mobiele aansluitingen in Nederland ook een data-abonnement heeft, heeft Tele2 bijna 250.000 mobiele abonnees met data-abonnement. Dit resulteert in een marktaandeel van 2,4 procent.

OPTA heeft in mei en juni 2011 onderzoek uitgevoerd onder de vier grootste mobiele netwerkaanbieders in Nederland (KPN, Vodafone, T-Mobile en Tele2) naar de vraag of en zo ja, hoe deze partijen hun dataverkeer analyseren. OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van het Samenwerkingsprotocol CBP-OPTA van 12 juli 2005.

Bevoegdheid CBP

Volgens artikel 51, eerste lid, van de Wbp ziet het CBP toe op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Op grond van artikel 61, eerste lid, van de Wbp zijn met het toezicht op de naleving belast de leden van het College en de ambtenaren van het secretariaat van het College.

Artikel 51, eerste lid, van de Wbp brengt tot uitdrukking dat de toezichthoudende taak van het CBP niet is beperkt tot het terrein van de Wbp, maar zich ook uitstrekt tot andere wetten, algemene maatregelen van bestuur en andere regelingen op grond waarvan persoonsgegevens worden verwerkt. Het CBP ziet aldus toe op de naleving van de bepalingen van de Wbp en van hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegeven in de sector elektronische communicatie.⁸

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.”⁹

De bevoegdheid tot het instellen van een onderzoek wordt ontleend aan artikel 60, eerste lid, van de Wbp.

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

⁸ Kamerstukken II 2002/03, 28 851, nr. 7, p. 53-54.

⁹ 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.

van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.

Daarnaast is Agentschap Telecom, onderdeel van het ministerie van Economische Zaken (hierna: Agentschap Telecom), op grond van artikel 15.1, eerste lid, onder c, h, j en k, van de Tw belast met het toezicht op de naleving van het bepaalde bij of krachtens de Tw, voor zover het onder andere betreft de bepalingen die betrekking hebben op prioritering van alarmnummers als bedoeld in artikel 7.7, derde of vierde lid, het gebruik van verkeersgegevens en locatiegegevens als geregeld in artikel 11.5, artikel 11.5a onderscheidenlijk artikel 11.13, buitengewone omstandigheden als geregeld in hoofdstuk 14 en verdere onderwerpen als bedoeld in de artikelen 11a.1 en 11a.2 (nieuw).¹⁰ De ACM is op grond van artikel 15.1, derde lid, van de Tw belast met het toezicht op de naleving van het bepaalde bij of krachtens andere bepalingen van de Tw en de bepalingen van de roamingverordening, voor zover voor dit onderzoek van belang.

Onderzoeksvragen

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

- Zijn de gegevens over en uit het mobiele dataverkeer die KPN verzamelt en verwerkt persoonsgegevens, zoals gedefinieerd in artikel 1, aanhef en onder a, van de Wbp?
- Zijn de doeleinden waarvoor KPN deze gegevens over en uit het dataverkeer verzamelt welbepaald, uitdrukkelijk omschreven en gerechtvaardigd als bedoeld in artikel 7 van de Wbp?
- Is er een grondslag voor de verwerking van deze gegevens over en uit het dataverkeer door KPN als bedoeld in artikel 8 van de Wbp?
- Heeft KPN de betrokkenen (tijdig) geïnformeerd over de gegevensverwerking, zoals bepaald in artikel 34 van de Wbp?
- Heeft KPN de verwerking van deze gegevens over en uit het dataverkeer bij het CBP gemeld in de zin van artikel 27 jo. 28 van de Wbp?

Verloop onderzoek

OPTA heeft in mei 2011 onderzoek (een quick scan) ingesteld onder de vier grootste mobiele netwerkaanbieders (KPN, Vodafone, T-Mobile en Tele2) naar de vraag of de manier waarop de mobiele netwerkaanbieders datapakketten analyseren strijdig is met bepalingen uit de Tw.¹¹

¹⁰ Zie artikel 2 van het Besluit aanwijzing toezichthouders Telecommunicatiewet (*Stb.* 2012, 11530). Artikel 1, derde lid, van de Samenwerkingsovereenkomst Agentschap Telecom - CBP van 15 september 2009 bepaalt, voor zover voor dit onderzoek van belang, dat indien het CBP tijdens onderzoeken in een ander kader op overtredingen van de Tw jo. de Wet bewaarplicht telecommunicatiegegevens stuit, het CBP zelfstandig onderzoek kan verrichten.

¹¹ 'Voorlopige bevindingen OPTA over gebruik Deep Packet Inspection', Mededeling OPTA 30 juni 2011. URL: <https://www.acm.nl/nl/publicaties/publicatie/10233/Voorlopige-bevindingen-OPTA-over-gebruik-Deep-Packet-Inspection/> (URL laatst bezocht op 29 mei 2013).

OPTA heeft op 30 juni 2011 haar voorlopige bevindingen gepubliceerd.¹²

OPTA heeft haar onderzoeksmateriaal naar de vraag of de manier waarop KPN, Vodafone, T-Mobile en Tele2 datapakketten analyseren strijdig is met bepalingen uit de Tw aan het CBP verstrekt (ontvangen op 5 juli 2011). OPTA heeft de gegevens en inlichtingen verstrekt op grond van artikel 10, eerste en derde lid, van het Samenwerkingsprotocol CBP-OPTA van 12 juli 2005 jo. artikel 24, tweede lid, van de Wet OPTA.

Het CBP heeft ambtshalve onderzoek ingesteld bij de vier mobiele aanbieders KPN, Vodafone, T-Mobile en Tele2.

Bij brief van 18 augustus 2011 heeft het CBP schriftelijk inlichtingen ingewonnen bij KPN. KPN heeft de gevraagde inlichtingen op 1 september 2011 aan het CBP verstrekt.

Het Landelijk Parket van het Openbaar Ministerie (hierna: OM) heeft medio 2011 oriënterend onderzoek verricht naar de mogelijk strafbare toepassing van data-analyse technieken (DPI) door KPN. Het onderzoeksmateriaal van het OM is op 15 september 2011 aan het CBP verstrekt.

Bij brief van 11 oktober 2011 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij KPN. KPN heeft de gevraagde inlichtingen aan het CBP verstrekt bij brief van 17 oktober 2011 (door het CBP ontvangen op 18 oktober 2011).

Op 3 november 2011 heeft het CBP mondeling (bevestigd per e-mail) twee stukken die ontbraken bij het onderzoeksmateriaal van OPTA, bij KPN opgevraagd. KPN heeft de stukken bij brief van 7 november 2011 aan het CBP verstrekt.

Op 10 november 2011 heeft het CBP mondelinge inlichtingen ingewonnen bij KPN.

Op 2 december 2011 heeft het CBP mondeling inlichtingen ingewonnen bij KPN. KPN heeft de gevraagde inlichtingen bij brief van 7 december 2011 aan het CBP verstrekt.

Op 9 december 2011 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij KPN. KPN heeft de gevraagde inlichtingen op 15 december 2011 aan het CBP verstrekt.

Het CBP heeft op 12 januari 2012 het rapport voorlopige bevindingen vastgesteld. Het CBP heeft KPN bij brief van 13 januari 2012 in de gelegenheid gesteld om haar zienswijze op het rapport voorlopige bevindingen naar voren te brengen. KPN heeft bij brief van 23 januari 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 24 februari 2012. Het CBP heeft bij brief van 27 januari 2012 het door KPN gevraagde uitstel verleend. KPN heeft haar zienswijze op 24 februari 2012 schriftelijk ingebracht.

¹² Idem.

Op 23 maart 2012 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij KPN. KPN heeft de gevraagde inlichtingen op 11 april 2012 aan het CBP verstrekt.

Op 31 mei en 12 juni 2012 heeft het CBP de wetsuitleg/-toepassing in het Conceptrapport definitieve bevindingen waar het gaat om artikelen uit de Tw afgestemd met het Agentschap Telecom respectievelijk OPTA.

Op 4 juni 2012 heeft KPN haar nieuwe privacy statements en (kopieën van haar) gewijzigde meldingen bij het CBP aan het CBP verstrekt.

Op 11 juni 2012 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en de advocaat-gemachtigde van KPN over het onderzoek.

Het CBP heeft op 21 augustus 2012 het Conceptrapport definitieve bevindingen vastgesteld. In verband met de technische complexiteit van het onderwerp van het onderzoek en de aanpassing van de bevindingen ten aanzien van het toepasselijk wettelijk kader heeft het CBP besloten in dit specifieke geval, in afwijking van haar reguliere werkwijze, concept definitieve bevindingen vast te stellen.

Het CBP heeft KPN bij brief van 21 augustus 2012 in de gelegenheid gesteld om haar zienswijze op het Conceptrapport definitieve bevindingen naar voren te brengen. KPN heeft bij brief van 19 september 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 9 oktober 2012. Het CBP heeft bij brief van 20 september 2012 het door KPN gevraagde uitstel verleend. KPN heeft haar zienswijze op 9 oktober 2012 schriftelijk ingebracht.

Op 7 december 2012 heeft telefonisch overleg plaatsgevonden tussen een medewerker van het CBP en de advocaat-gemachtigde van KPN over het onderzoek.

Op 19 december 2012 heeft het CBP een vordering om inlichtingen en inzage in zakelijke stukken en bescheiden aan KPN gezonden.

Op 3 januari 2013 heeft KPN per e-mail contact opgenomen over het onderzoek.

KPN heeft bij brief van 7 januari 2013 verzocht om uitstel van de termijn voor het geven van een reactie op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden tot en met 25 januari 2013. Het CBP heeft bij brief van 9 januari 2013 uitstel verleend tot en met 21 februari 2013.

Op 22 en 24 januari 2013 heeft KPN per e-mail contact opgenomen over het onderzoek.

Op 28 januari 2013 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en de advocaat-gemachtigden van KPN over een door KPN verkozen anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer.

Op 31 januari 2013 heeft het CBP schriftelijke inlichtingen ingewonnen bij KPN over de anonimiseringsoplossing. KPN heeft de gevraagde inlichtingen op 6 februari 2013 aan het CBP verstrekt.

Op 11 februari 2013 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij KPN over de anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer. Op 14 februari 2013 heeft KPN per e-mail contact opgenomen over het onderzoek. KPN heeft de gevraagde inlichtingen op 15 februari 2013 aan het CBP verstrekt.

Op 16 en 17 februari 2013 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en de advocaat-gemachtigde van KPN over de anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer.

KPN heeft op 19 februari 2013 verzocht om uitstel van de termijn voor het geven van een reactie op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden tot en met 27 februari 2013. Het CBP heeft bij brief van 21 februari 2013 uitstel verleend tot en met 28 februari 2013. Het CBP heeft in deze brief ook gereageerd op de anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer.

KPN heeft bij brief van 28 februari 2013 gereageerd op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden.

Op 10 april 2013 heeft KPN per e-mail contact opgenomen over het onderzoek.

Op 15 april 2013 heeft het CBP KPN telefonisch geïnformeerd over de planning van het onderzoek.

Op 23 en 27 mei 2013 heeft het CBP de wetsuitleg/-toepassing in dit rapport waar het gaat om artikelen uit de Tw afgestemd met de ACM respectievelijk het Agentschap Telecom.

Het CBP heeft op 29 mei 2013 het rapport definitieve bevindingen vastgesteld.

Zienswijze van KPN op de voorlopige bevindingen van het CBP van 12 januari 2012

In haar zienswijze van 24 februari 2012 op het Rapport voorlopige bevindingen van het CBP (hierna: Zienswijze 1) brengt KPN, samengevat weergegeven, naar voren dat de gegevensverwerking door aanbieders van telecommunicatienetwerken en -diensten wordt geregeerd door de Tw. De Wbp is aanvullend van toepassing voor zover onderwerpen niet (uitputtend) worden geregeld door de Tw.

KPN geeft aan dat de gegevens die KPN verwerkt door middel van toepassing van data-analyse technieken uitsluitend verkeersgegevens betreffen en niet de inhoud van communicatie (met uitzondering van geautomatiseerde scans door firewalls, virusscanners en spamfilters).

De doeleinden waarvoor KPN deze verkeersgegevens verwerkt, vallen volgens KPN binnen de wettelijke grondslagen in de Tw voor de verwerking van verkeersgegevens en voldoen overigens ook aan het proportionaliteitsvereiste dat in deze grondslagen is vevat.

KPN wijst erop dat de door het CBP aangedragen technische alternatieven voor data-analyse geen reële alternatieven zijn. Het rapport voorlopige bevindingen is overigens ook onzorgvuldig voorbereid en ontoereikend gemotiveerd.

Doordat KPN de verkeersgegevens niet aanwendt om het gebruik van het netwerk door personen te bepalen of anderszins om een persoon te beoordelen of anders te behandelen, betreffen deze gegevens volgens KPN geen persoonsgegevens in de zin van de Wbp, zodat voor aanvullende toepassing van de bepalingen van de Wbp geen plaats is.

KPN geeft aan dat zij op eigen initiatief aanleiding heeft gezien om haar privacy statements voor abonnees ter verduidelijking aan te passen.

In **bijlage V** bij dit rapport is de zakelijke inhoud van de zienswijze 1 van KPN opgenomen per onderdeel (met de toevoeging '**Zienswijze 1 KPN**'), met de reactie daarop van het CBP. Deze bijlage vormt een integraal onderdeel van dit rapport.

Zienswijze van KPN op de concept definitieve bevindingen van het CBP van 21 augustus 2012

In haar zienswijze van 9 oktober 2012 op het CBP Conceptrapport definitieve bevindingen (hierna: Zienswijze 2) (daaronder in dit geval mede begrepen de daaropvolgende correspondentie als beschreven onder het kopje 'Verloop onderzoek', p. 9 e.v. van dit rapport) brengt KPN, samengevat weergegeven, ten eerste naar voren dat zij heeft besloten de data-analyse tools voor netwerkmanagement ([VERTROUWELIJK: apparatuur]) en het afrekenen van prepaidverkeer ([VERTROUWELIJK: apparatuur]) stop te zetten en gestopt te houden, behoudens nader tegenbericht. KPN geeft in haar zienswijze 2 verder aan alle via de [VERTROUWELIJK: apparatuur] opgeslagen data én de geanonimiseerde [VERTROUWELIJK: apparatuur]-data die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening, te verwijderen. KPN is daarnaast in overleg getreden met de leverancier van de [VERTROUWELIJK: apparatuur], het [VERTROUWELIJK] bedrijf [VERTROUWELIJK] voor het ontwikkelen en uitbrengen van een technisch alternatief dat ervoor zorgt dat verkeersgegevens zo snel mogelijk onomkeerbaar worden geanonimiseerd (KPN acht zo'n alternatief op dit moment proportioneel). Als alternatief voor de data-analyse functionaliteit van de [VERTROUWELIJK: apparatuur] verleent KPN thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK], op zo'n manier dat [VERTROUWELIJK].

Ten tweede brengt KPN een aantal opmerkingen en aanvullingen van feitelijke aard naar voren ten aanzien van de werking van de door KPN ingezette data-analyse tools en de verwachte groei van het signaleringsverkeer.

Ten derde betoogt KPN dat het CBP slechts bevoegd is om de bepalingen van hoofdstuk 11 en 13 van de Tw toe te passen, en dan nog alleen voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie.

Ten vierde betoogt KPN dat (i) uit de Europese wetgeving blijkt dat de Privacyrichtlijn alleen geldt in die gevallen waarin de e-Privacyrichtlijn geen specifieke regeling bevat,

(ii) de wetsgeschiedenis bij de Wbp en de Tw uitdrukkelijk stelt dat de Tw op onderdelen een specialis is ten opzichte van de Wbp en (iii) de Tw (aldus) een uitputtende regeling geeft voor de verwerking van verkeersgegevens en communicatie, die ook persoonsgegevens zijn/is. KPN geeft in haar zienswijze 2 overigens aan dat toetsing aan louter de grondslagen in de Tw, zoals voorgestaan door KPN, (op een enkel onderdeel na) niet leidt tot een drastisch andere uitkomst dan *“de toetsing door het CBP aan de grondslagen in de Wbp”*.

Ten vijfde betoogt KPN dat URL's verkeersgegevens in plaats van communicatie zijn.

Ten zesde maakt KPN een aantal opmerkingen van juridische aard ten aanzien van de mogelijke grondslagen voor de inzet van data-analyse tools voor prepaid facturering en inkomende spam.

Ten zevende brengt KPN naar voren dat ook de overige door het CBP geconstateerde overtredingen - ten aanzien van verdere verwerking, informatieplicht, doelomschrijving en meldingsplicht - zijn beëindigd, doordat KPN heeft besloten de data-analyse tools voor netwerkmanagement en het afrekenen van prepaidverkeer stop te zetten en gestopt te houden.

Ten achtste maakt KPN bezwaar tegen het labelen van de verdere verwerking ten behoeve van analyse van de eigen dienstverlening als voor marketingdoeleinden.

Ten slotte heeft KPN het CBP nadere inlichtingen verstrekt omtrent de door [VERTROUWELIJK] geoffreerde en door KPN voorgestelde anonimiseringsoplossing die KPN voornemens is te implementeren, waarin [VERTROUWELIJK].

In **bijlage VI** bij dit rapport is de zakelijke inhoud van de zienswijze 2 van KPN opgenomen per onderdeel (met de toevoeging '**Zienswijze 2 KPN**'), met de reactie daarop van het CBP en of de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies. Deze bijlage vormt een integraal onderdeel van dit rapport.

2. FEITELIJKE BEVINDINGEN

2.1 Organisatiebeschrijving

KPN, gevestigd en kantoorhoudende te Den Haag, is opgericht op 1 januari 1989 en ingeschreven bij de Kamer van Koophandel onder nummer 27124701. De doelomschrijving van KPN is: *“Het uitoefenen van activiteiten in de ruimste zin op het gebied van de telecommunicatie, alsmede holding- en financieringsmaatschappij. De vennootschap maakt deel uit van de groep van Koninklijke KPN N.V. Bij het uitoefenen van haar onderneming richt de vennootschap zich mede naar het belang van deze groep.”*

KPN is geregistreerd bij de ACM als aanbieder van een openbare elektronische communicatiedienst en -netwerk.¹³

KPN is de algemene marktleider mobiele telefonie in Nederland met (eind 2012) een marktaandeel van ongeveer 30-35% van de mobiele aansluitingen.¹⁴ Volgens cijfers op haar eigen website had KPN per 31 december 2011 een marktaandeel mobiele telefonie van ~45%, en 10 miljoen mobiele klanten in Nederland. Uit de cijfers van KPN over het laatste kwartaal van 2010 blijkt dat 40% van de KPN abonnees¹⁵ een (prepaid of postpaid) data abonnement heeft (omgerekend ongeveer 3,8 miljoen aansluitingen).¹⁶ Binnen KPN heeft Hi, een handelsnaam van KPN, het grootste aantal smartphone gebruikers.¹⁷

KPN heeft de verwerking van persoonsgegevens, voor zover voor dit onderzoek van belang, op 3 september 2010 (gewijzigd) gemeld bij het CBP onder nummer m1321211 (versienummer 3.0).

¹³ URL:

<https://www.acm.nl/nl/onderwerpen/telecommunicatie/registraties/geregistreerde-ondernemingen/resultaat/?query=>

¹⁴ Volgens gegevens uit de Openbare rapportage mobiel Q4 2012 van de ACM had KPN aan het einde van het vierde kwartaal van 2012 een marktaandeel van 30-35% van de mobiele retailaansluitingen. Bron tabel 'Mobiel: Marktaandelen retail aansluitingen' uit de ACM Openbare rapportage mobiel Q4, p. 1, URL:

<https://www.acm.nl/nl/download/bijlage/?id=10942> (URL laatst bezocht op 29 mei 2013). Vgl. Marktrapportage Elektronische Communicatie December 2011, Delft: TNO 2011, p. 15. URL: <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/01/18/marktrapportage-elektronische-communicatie.html>.

Volgens cijfers op haar eigen website had KPN per 31 december 2011 een marktaandeel mobiele telefonie van ~45%, en 10 miljoen mobiele klanten in Nederland. URL: <http://www.kpn.com/corporate/overkpn/Bedrijfsprofiel/het-bedrijf/kernfeiten.htm> en <http://www.kpn.com/v2/static/annualreport-2012/wie-we-zijn-en-wat-we-doen/index.html>.

¹⁵ Daaronder mede begrepen de merken Telfort en Hi.

¹⁶ TNO-rapport. Marktrapportage Elektronische Communicatie December 2011, Delft: TNO 2011, p. 56. Zie ook Jaarverslag 2012 OPTA, p. 7: *“Ruim 45 procent van de aansluitingen voor mobiele telefoons wordt ook gebruikt voor internet.”*

¹⁷ ‘Smartphone-penetratie stijgt naar 42 procent in Nederland’, *Telecompaper* 4 augustus 2011.

In de melding waren, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

‘Gegevens klanten en gebruikers elektronische communicatiediensten KPN’
(m1321211)

Het technisch mogelijk maken van de dienstverlening, waaronder het opbouwen van verbindingen.
Het beheer van de relatie tussen KPN en de klant waaronder alle activiteiten in verband met de voorbereiding en de uitvoering van de tussen KPN en de klant gesloten overeenkomsten.
Beheer van de relatie met de klant, waaronder notanavraag, klachtafhandeling, storingsopheffing, advisering, e.d.
Het factureringsproces, waaronder notanavraag, klachtafhandeling, storingsopheffing, advisering, e.d.
Netwerkmanagement, waaronder netwerkplanning en netwerkarchitectuur, netwerkintegriteit en fraudedetectie.
Verwerking t.b.v. een verantwoorde bedrijfsvoering, waaronder beveiliging, risicobeperking, integriteitsonderzoek, behandeling van ongewenste oproepen, uitbreiding en verbetering van dienstverlening.
Het verwerken van persoonsgegevens (ook na contractsbeëindiging) t.b.v. marktonderzoek en marketing- en verkoop van dienstverlening van KPN en haar groepsmaatschappijen, o.m. voor het doen van gezamenlijke aanbiedingen. ¹⁸

KPN heeft verklaard dat de melding met nummer m1321211 betrekking heeft op de verwerking van gegevens over en uit het dataverkeer bij de inzet van data-analyse technieken ten behoeve van (i) routeren van MMS- en prepaidverkeer, (ii) klachtafhandeling en (iii) netwerkmanagement, netwerkplanning en netwerkarchitectuur.¹⁹

KPN heeft geen andere meldingen gedaan die betrekking hebben op de verwerking van gegevens over en uit het dataverkeer bij de inzet van data-analyse technieken in haar mobiele netwerk. KPN heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.

Getroffen maatregelen: gewijzigde melding

KPN heeft de melding met nummer m1321211 op 9 maart 2012 (door het CBP ontvangen op 12 maart 2012) gewijzigd (versienummer 4.0).

¹⁸ In de melding waren, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens onder andere genoemd: ‘Contractanten en gebruikers van elektronische communicatiediensten van KPN’ respectievelijk ‘NAWT-gegevens’, ‘Afgenomen diensten’, ‘Verkeersgegevens, incl. gebruiksgegevens, surfgedrag, kijkgedrag, IP-adres, URL’.

¹⁹ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 7.

In de gewijzigde melding zijn, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

‘Gegevens klanten en gebruikers elektronische communicatiediensten KPN’
(m1321211)

Het technisch mogelijk maken van de dienstverlening, waaronder het opbouwen van verbindingen.
Het beheer van de relatie tussen KPN en de klant waaronder alle activiteiten in verband met de voorbereiding en de uitvoering van de tussen KPN en de klant gesloten overeenkomsten.
Beheer van de relatie met de klant, waaronder notanavraag, klachtafhandeling, storingsopheffing, advisering, e.d.
Het factureringsproces inclusief facturering van prepaid en MMS-diensten, waaronder notanavraag, klachtafhandeling, storingsopheffing, advisering.
Netwerkmanagement, waaronder netwerkbeheer, netwerkplanning, netwerkarchitectuur, fraudedetectie en bevordering van netwerkintegriteit en -continuïteit (zoals het beveiligen van het KPN netwerk tegen veiligheidsinbreuken, spam en malware).
Verwerking t.b.v. een verantwoorde bedrijfsvoering, waaronder beveiliging, uitbreiding en verbetering van het netwerk en de dienstverlening.
Het verwerken van persoonsgegevens (ook na contractsbeëindiging) t.b.v. marktonderzoek en marketing- en verkoop van dienstverlening van KPN en haar groepsmaatschappijen, o.m. voor het doen van gezamenlijke aanbiedingen. ²⁰

2.2 Mobiel netwerk, netwerkverkeer en plaatsing data-analyse apparatuur

Het mobiele netwerk van KPN bestaat uit een GSM-gedeelte (voor de afhandeling van spraakverkeer) en een GPRS/UMTS-gedeelte (voor de afhandeling van dataverkeer). Deze gedeeltes staan in verbinding met elkaar. Mobiele apparaten, zoals smartphones gebruiken beide gedeeltes van het netwerk, al naar gelang de gebruikte dienst (spraak of data).

Het mobiele netwerk is daarnaast verder te verdelen in een radiotoegangsnetwerk- en een core-netwerkgedeelte (zie **bijlage I**). Het mobiele netwerk van KPN vervoert niet alleen spraak- en dataverkeer, maar ook signaleringsverkeer (kleine berichten die nodig zijn om de verbinding op te bouwen, in stand te houden en te verbreken). Spraak-, data- en signaleringsverkeer maken gebruik van dezelfde radioweg (toegang

²⁰ In de gewijzigde melding waren, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens onder andere genoemd: ‘Contractanten en gebruikers van elektronische communicatiediensten van KPN’ respectievelijk ‘NAWT-gegevens’, ‘Afgenomen diensten’, ‘Verkeersgegevens die verwerkt worden in het netwerk van KPN bij het vervoer van communicatie over het netwerk en facturering daarvan, maar die niet de inhoud van de communicatie zelf betreffen, zoals (i) telefoniegegevens waaronder datum en tijdstip van aanvang en einde verbinding, soort dienst, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), locatiegegevens en (ii) internetgegevens waaronder gebruikersidentificatie, datum en tijdstip van de log-in en log-off van een internet sessie, de applicatieserver waarmee een app verbinding maakt, internetdienst, e-maildienst of internettelefoniedienst, IP-adres, soort internetdienst’.

tot het radiotoegangsnetwerk). Elk onderdeel van het mobiele netwerk heeft een maximum capaciteit (zie ook het kopje 'Achtergrond onderzoek', p. 6 van dit rapport).

KPN licht in haar zienswijze 1 nader toe dat de smartphone via de radioweg in verbinding staat met een van de [VERTROUWELIJK] Base Stations van het KPN [VERTROUWELIJK]. De Base Stations staan in verbinding met een van de [VERTROUWELIJK] Base Station managers voor dataverkeer (Radio Network Controller). De Radio Network Controller zorgt er volgens KPN voor dat het dataverkeer zo snel, efficiënt en veilig mogelijk wordt vervoerd (onder andere door radiocapaciteit slim te alloceren en te reserveren wanneer de gebruiker inlogt en dataverkeer te vervoeren via het dichtstbijzijnde Base Station). De Base Stations en de Radio Network Controllers vormen samen het GPRS/UMTS-gedeelte van het toegangsnetwerk. De Radio Network Controller staat in verbinding met een van de [VERTROUWELIJK] Serving GPRS Support Nodes (SGSN). De SGSN (a) fungeert als centrale en (b) is verantwoordelijk voor de protocolconversie van het radioprotocol dat vanuit het radionetwerk binnenkomt naar een IP-protocol (GPRS Tunnelling Protocol; GTP), opdat het dataverkeer zijn weg kan vervolgen naar het internet. De SGSN is gekoppeld aan het Home Location Register (databank waarin onder meer het IMSI, het MSISDN en de mobiele (prepaid of postpaid) datadiensten waar de abonnee op is geabonneerd, zijn opgeslagen) en het Visitor Location Register (databank waarin de actuele locaties van de gebruikers worden bijgehouden), en staat in verbinding met een van de [VERTROUWELIJK] Gateway GPRS Support Nodes (GGSN). De GGSN zorgt ervoor dat dataverkeer van en naar externe netwerken zoals het internet of een intranet wordt vervoerd, wijst IP-adressen voor inkomend en uitgaand dataverkeer toe en verzorgt de administratie voor de facturering van het dataverkeer. [VERTROUWELIJK].²¹

KPN maakt gebruik van data-analyse technieken op het dataverkeer (inclusief signaleringsverkeer) in haar mobiele netwerk.²² Daartoe zijn op verschillende punten in het netwerk verschillende soorten data-analyse apparatuur geplaatst, onder andere [VERTROUWELIJK].²³

Met gebruikmaking van de data-analyse apparatuur inspecteert en analyseert KPN *headers*, en soms de inhoud van het mobiele dataverkeer (dit laatste alleen voor spam- en virusfiltering; zie p. 38 e.v. van dit rapport). Daartoe worden datapakketten door/langs een filter met inspectieregels geleid. Voor het doeleinde netwerkplanning en -beheer is de data-analyse gestaakt op 21 september 2012, en voor het doeleinde van prepaidverkeer is de data-analyse gestaakt op 3 oktober 2012.

Alle dataverkeer (inclusief signaleringsverkeer) dat over het netwerk wordt verzonden, is ingedeeld in datapakketten (*packets*). Een packet bevat twee soorten informatie: headers (adresseringsgegevens op de 'envelop') en inhoud van het verkeer/payload (de 'brief').

²¹ Zienswijze 1 KPN van 24 februari 2012, p. 28-30.

²² Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 1-2. Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2-3.

²³ Zienswijze 1 KPN van 24 februari 2012, p. 38-39.

KPN verkrijgt via de data-analyse apparatuur²⁴ gegevens over en (in een enkel geval) uit het dataverkeer van (potentieel)²⁵ alle²⁶ ongeveer 3,8 miljoen KPN abonnees met een (prepaid of postpaid) data abonnement en van de gebruikers van haar dataverkeersdiensten. KPN licht in haar zienswijze 2 nader toe dat of de inzet van data-analysetools impact heeft op de privacy van eindgebruikers afhangt van het doel waarvoor data-analyse wordt toegepast en de wijze waarop de data-analysetools worden ingericht. Data-analysetools ‘zien’ of verwerken niet meer dan dat waarvoor ze zijn ingesteld.²⁷

Van het totaal aantal actieve KPN dataverbruikers hebben er volgens cijfers van KPN [VERTROUWELIJK] een prepaid aansluiting.²⁸ Van deze [VERTROUWELIJK] prepaid abonnees heeft KPN van [VERTROUWELIJK] van de IOM (Internet Op Je Mobiel) prepaid abonnees NAW-gegevens en/of e-mailadressen. KPN heeft van [VERTROUWELIJK] van de IOL (Internet Op Je Laptop) prepaid abonnees NAW-gegevens en/of e-mailadressen.²⁹

De gegevens ‘over’ en ‘uit’ het dataverkeer (inclusief signaleringsverkeer) worden hier, ter illustratie, beschreven aan de hand van de verschillende lagen van het ISO-OSI-model (hierna: OSI-model) en het TCP-IP model. Beide modellen zijn een gestandaardiseerde indeling van netwerkverkeer in respectievelijk zeven en vijf lagen. De OSI-lagen zijn van laag naar hoog: fysieke, link-, netwerk-, transport-, sessie-, presentatie- en applicatielaag. In beide modellen bevat een packet in elke laag headers.

²⁴ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 6 en bijlage 2 bij deze reactie.

²⁵ Dat wil zeggen: onder andere afhankelijk van de apps die zij op hun smartphones hebben staan.

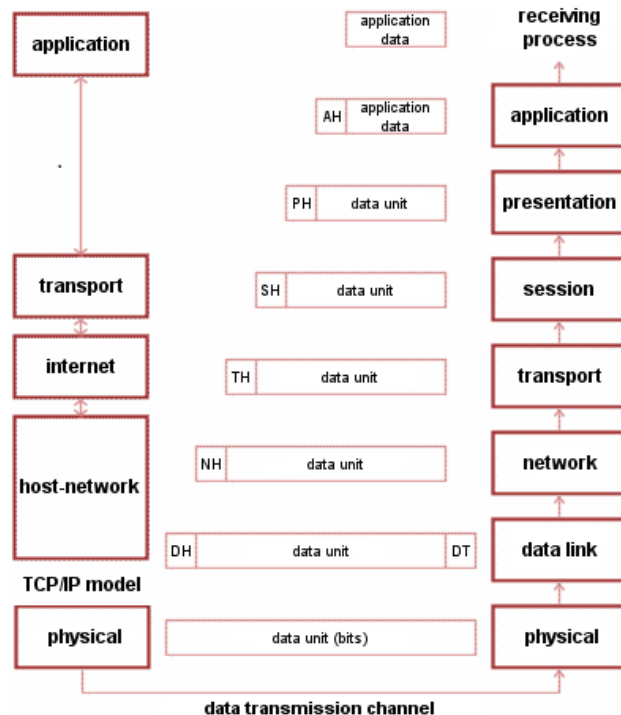
²⁶ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 4: “Bij de inzet van packet inspection wordt geen onderscheid gemaakt tussen categorieën van betrokkenen.” Idem, p. 4: “Om die [te weten: de Hi abonnees, toevoeging door het CBP] te selecteren werden door de retailorganisatie wel de IMSI-nummerreeksen van Hi klanten gebruikt om uit de totale analyse de relevante gegevens te selecteren”, (onderstreping toegevoegd door het CBP). Idem, p. 4-5: “Om ervoor te zorgen dat het door KPN klanten richting Internet gestuurde verkeer zo goed mogelijk geschoond wordt van malware of spam, worden malware- of spamfilters toegepast op de totale verkeersstroom richting Internet”, (onderstreping toegevoegd door het CBP).

²⁷ Zienswijze 2 KPN, p. 7-8.

²⁸ Bijlage bij reactie KPN op verzoek om inlichtingen van 11 april 2012, p. 1.

²⁹ Reactie KPN op verzoek om inlichtingen van 11 april 2012, p. 1. KPN heeft verklaard dat zij voornamelijk identificerende gegevens ontvangt van prepaid abonnees die hun gegevens via de websites van de verschillende merken van KPN (Hi, KPN en Telfort) opgeven om extra beltegoed te krijgen. Idem, p. 1-2.

AFBEELDING I Opbouw packets volgens TCP-IP en OSI-model³⁰



De headergegevens in lagen 2 tot en met 7 zijn in dit rapport gedefinieerd als gegevens ‘over’ het dataverkeer. Het bestemmings- en afzender-IP-adres zitten in laag 3/4. Dit kan technisch worden gezien als de adressering op de ‘buitenste envelop’: gegevens die noodzakelijk zijn om het verkeer op de bestemming af te leveren. Vanaf laag 4 (transportlaag) bevatten de headers gedetailleerde informatie over gebruikte apps en bezochte websites, zoals het gebruikte protocol, de frequentie (het aantal keren dat verbinding wordt gemaakt) en de *hostname* (URL op hoofddomein). Inhoud van het verkeer/payload is in dit rapport gedefinieerd als gegevens ‘uit’ het dataverkeer.

Het CBP merkt op dat het OSI-model hier niet wordt gebruikt als een normatief model dat voorschrijft op welke wijze een telecommunicatienetwerk moet zijn ingericht en ook niet ter onderbouwing van een (juridische) kwalificatie van de gegevens over en uit het dataverkeer, maar als hulpmiddel om processen en gegevensstromen in een netwerk te kunnen aanduiden. De omstandigheid dat zo’n model altijd een vereenvoudiging is van de werkelijkheid, doet niet af aan de waarde daarvan als hulpmiddel. Ter vergelijking is tevens de indeling van netwerkverkeer in het TCP-IP model opgenomen in dit rapport.

2.3 Overzicht doeleinden

KPN verklaart dat er (limitatief) vier doeleinden zijn voor de toepassing van data-analyse technieken in haar mobiele netwerk. De vier doeleinden zijn:

³⁰ Bron: URL: http://www2.themanualpage.org/networks/networks_osi2.php3 (URL laatst bezocht op 29 mei 2013).

1. Netwerkplanning en -beheer. Om inzicht te hebben/krijgen in de ontwikkelingen van verkeer, netwerkgebruik etc. in verband met de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps. ³¹
2. Facturering van MMS- en prepaidverkeer. Om MMS-verkeer (waarvoor een vast tarief geldt per bericht) buiten databundels te kunnen factureren, en voor de routing van prepaidverkeer naar opwaardeersites en tarifiering (zodat prepaid abonnees ook zonder saldo hun tegoed kunnen opwaarderen). ³²
3. Voor het gebruik van firewalls, spamfilters en virusscanners. ³³
4. Behandeling van klantklachten. Als moet worden gekeken waarom bepaalde routeringen niet goed functioneren. ³⁴

Tevens verstrekke KPN vanaf februari 2011 tot september 2012 rapportages over (de toename van) het gebruik van allerlei apps aan het KPN retailbedrijf ten behoeve van marktonderzoek (analyse van de eigen dienstverlening).³⁵

Hierna worden achtereenvolgens beschreven de gegevensverwerkingen voor de hierboven genoemde vier doeleinden, en de verstrekking door KPN van gegevens over het dataverkeer aan het KPN retailbedrijf ten behoeve van analyse van de eigen dienstverlening (zie paragraaf 2.8, p. 43 e.v. van dit rapport).

2.4 Netwerkplanning en -beheer

Als eerste verzamel- en verwerkingsdoeleinde van gegevens noemt KPN netwerkplanning en -beheer (daaronder mede begrepen het voorkomen van congestie).³⁶

Aanleiding toepassing data-analyse technieken

KPN verklaart dat het verkrijgen van gegevens met betrekking tot het mobiele dataverkeer door middel van data-analyse technieken noodzakelijk is voor het doeleinde van netwerkplanning en -beheer *“om het effect van de explosieve toename van applicaties op het netwerk of meer specifiek de belasting op het signaleringsdeel daarvan in kaart te brengen en inzicht te krijgen in welke applicaties leiden tot veel signaleringen in het netwerk (...).”*³⁷

In haar zienswijze 1 voegt KPN daaraan toe dat het GSM-gedeelte en het GPRS-gedeelte in verbinding met elkaar staan, resources delen en in grote mate afhankelijk zijn van elkaar: *“Van belang hierbij is dat het mobiele KPN netwerk zowel voor belverkeer als*

³¹ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 1.

³² Idem.

³³ Idem.

³⁴ Idem, p. 2.

³⁵ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4 en reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5-6.

³⁶ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 1.

³⁷ Idem, p. 2. Zie ook reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4: *“Het is van belang om tijdig te constateren dat er aanpassingen in het netwerk moeten worden gedaan om het groeiend aantal signaleringen op te kunnen vangen. Daarvoor is nodig om inzicht te verkrijgen in welke applicaties leiden tot veel signaleringen in het netwerk en om trends in de ontwikkeling van het gebruik van applicaties in kaart te kunnen brengen.”*

*voor dataverkeer een maximumcapaciteit heeft. (...) Als dit maximum wordt overschreden, is er een risico dat het betreffende [GPRS-, toevoeging door het CBP] netwerkonderdeel crasht. (...) Indien dit tot gevolg heeft dat ook het radiotoegangsnetwerk crasht, zal ook niet meer mogelijk zijn om te bellen via het GSM-gedeelte.*³⁸

Mobiele apparaten, zoals smartphones (en daarop geïnstalleerde/gebruikte apps) maken ander(s) gebruik van het mobiele netwerk dan reguliere toestellen. Ze maken veel vaker contact met het internet, en gebruiken daarvoor telkens het signaleringskanaal (en het radiotoegangsnetwerk).³⁹ Zo laten verschillende apps mobiele apparaten veelvuldig contact zoeken met de dichtstbijzijnde zendmast(en), ook zonder dat het voor de abonnee duidelijk is dat er dataverkeer wordt uitgewisseld, om de verbinding met het internet 'open' te houden. Dit fenomeen wordt wel 'chatty apps' genoemd en leidt tot een significante toename van het signaleringsverkeer. Als het radiotoegangsnetwerk crasht als gevolg van teveel signaleringen in het GPRS/UMTS-gedeelte kan er ook niet meer worden gebeld.

KPN geeft aan dat zowel de verschillende typen smartphones als de apps zich onderling verschillend gedragen waar het de verhouding betreft tussen dataverkeer en signaleringen.⁴⁰

In haar brief aan het Landelijk Parket licht KPN toe: *"Voor traditionele diensten wordt iedere keer als een gesprek wordt opgezet, of een SMS wordt verstuurd, een signalering gedaan in het netwerk. Signalering wordt in de GSM standaard separaat gedaan en is noodzakelijk om inhoudelijke telecommunicatie te laten plaatsvinden. Signaleringsverkeer heeft daarom volgens de standaard prioriteit."*⁴¹ En: *"Normaal heeft 1 gebruiker die belt ook maar 1 sessie, maar met de smartphone applicaties heeft 1 gebruiker gemiddeld 10 sessies, en wordt dit ook nog eens de hele dag door gebruikt ipv alleen op het moment van bellen/browsen. Communicatie vindt ook onzichtbaar voor de gebruiker plaats. Vooral de radiosessies zijn bepalend in het kunnen bieden van de hele mobiele dienst, maar ook in de apparatuur die de IP verbinding verder transporteert moet op alle niveaus voldoende capaciteit hebben. Door de stijging van het aantal gelijktijdige sessies, moet er heel snel worden uitgebreid. Op dit moment is een smartphone gemiddeld tot wel [VERTROUWELIJK] zo actief als een gewone mobiele telefoon. Maar het eind is nog niet in zicht. Deze factor zou gemakkelijk nog vele malen kunnen stijgen door de vervanging van de grote hoeveelheid klanten met een smartphone en de actieve applicaties."*⁴²

De informatie over welke apps op welke smartphones (met welke besturingssystemen) leiden tot veel signaleringen in het netwerk is volgens KPN nodig om een voorspelling te kunnen doen van de benodigde capaciteit in het netwerk. KPN verklaart: *"Deze forecast moet i.v.m. met de doorlooptijd van uitbreidingen*

³⁸ Zienswijze 1 KPN van 24 februari 2012, p. 32; zie ook idem, p. 24-31.

³⁹ Vgl. o.a. Chris Foresman, 'How smartphones are bogging down some wireless carriers', *Ars technica* 22 februari 2010. URL: <http://arstechnica.com/gadgets/news/2010/02/how-smartphones-are-bogging-down-some-wireless-carriers.ars> (URL laatst bezocht op 29 mei 2013).

⁴⁰ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 2.

⁴¹ Brief KPN aan het Landelijk Parket van 25 mei 2011, p. 3.

⁴² Bijlage 2 - Gebruik van analysetechnieken door KPN bij brief KPN aan het Landelijk Parket van 25 mei 2011, p. 2. Zie ook bijlage 2 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

[VERTROUWELIJK] voorop lopen.”⁴³ In haar reactie op een verzoek om inlichtingen voegt KPN daaraan toe: *“Alleen op die manier is een goede planning van werkzaamheden en aanschaf van apparatuur op een (kosten-)efficiënte wijze te waarborgen. Als planningen korter worden zullen kosten toenemen (zowel voor inkoop bij toeleveranciers als de uitvoering van werkzaamheden) en nemen de risico’s op het te laat realiseren van de benodigde uitbreidingen toe.”*⁴⁴

KPN schrijft dat vanaf het derde kwartaal van 2010 de signaleringscapaciteit is [VERTROUWELIJK]. Het aantal RNC’s is sinds 2010 uitgebreid tot [VERTROUWELIJK]. Oude verwerkingstechnologie is vervangen door nieuwe en de verwerkingscapaciteit is [VERTROUWELIJK]. In totaal is volgens cijfers van KPN meer dan [VERTROUWELIJK] geïnvesteerd.⁴⁵

Volgens KPN kan niet worden volstaan met steekproefsgewijze controle:

*“het sampelen van verkeer, waarbij steekproefsgewijs naar de belasting van het netwerk wordt gekeken, is geen juiste methode om een reëel beeld te krijgen van de belasting van het netwerk, omdat daarbij de piekbelasting opgaat in een veel lagere gemiddelde belasting.”*⁴⁶

In haar reactie op een verzoek om inlichtingen over de vraag of de netwerkbelasting die smartphones en apps veroorzaken ook op andere manieren kan worden gemeten, licht KPN toe:

“Tot het uitvoeren van steekproeven in het netwerk - op een specifiek geselecteerde groep klanten - is niet overgegaan omdat de ontwikkeling van het gebruik van applicaties op het moment dat de keuzes werden gemaakt zo stormachtig en onvoorspelbaar waren (en nog zijn) dat het niet goed mogelijk is om een voldoende betrouwbare steekproef te definiëren. (...) Voor de noodzakelijke analyse is het niet goed mogelijk om gebruik te maken van andere middelen dan daadwerkelijke metingen/steekproeven. De combinatie van kwalitatief technisch onderzoek met extern marktonderzoek is niet in staat vergelijkbare (en betrouwbare) informatie te leveren als daadwerkelijke verkeersmetingen. Marktonderzoek naar het gebruik van

⁴³ Bijlage 3 - De inzet van [VERTROUWELIJK: apparatuur] bij brief KPN aan het Landelijk Parket van 25 mei 2011, p. 5. KPN licht toe dat *“in 2011 de capaciteit voor signalering is uitgebreid om voldoende capaciteit te hebben voor de migratie van het klantbestand naar smartphones. Hiervoor is bijv. tot nu toe dit jaar het aantal RNC’s al uitgebreid van [VERTROUWELIJK: (...)], het aantal SGSN’s uitgebreid met [VERTROUWELIJK: (...)] (en is een veel krachtiger type geïntroduceerd). Daarmee waren grote extra investeringen gemoeid. De noodzakelijke dimensionering van het netwerk was alleen mogelijk door onzekerheid over de oorzaken van de groei uit te sluiten, om zeker te weten dat de uitbreidingen tijdig zouden kunnen worden opgeleverd en dat de inspanningen op de juiste activiteiten werden ingezet.”* Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 2.

⁴⁴ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 2. Zienswijze 1 KPN, p. 33: *“Het KPN [VERTROUWELIJK] kan op piekbelastingmomenten inspringen door meer netwerkcapaciteit bij te schakelen of het netwerk op bepaalde punten verder uit te breiden.”* Daarbij kan worden gedacht aan situaties als tijdelijke grootschalige evenementen, zoals de Elfstedentocht.

⁴⁵ Zienswijze 1 KPN, p. 37-38.

⁴⁶ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 4.

nieuwe applicaties heeft grote beperkingen, omdat het (i) ver achter de ontwikkelingen aanloopt (ii) er bij marktonderzoeken vaak conclusies moeten worden getrokken op basis van relatief kleine steekproeven, (iii) het voor grote groepen klanten zeer moeilijk is om een voldoende heldere vraagstelling te formuleren om betrouwbare antwoorden te krijgen en (iv) bestaande onderzoeken niet in staat zijn het feitelijk gebruik te meten, maar slechts het aantal malen dat een applicatie is gedownload.”⁴⁷

Desgevraagd verklaart KPN dat een alternatieve vorm van data-analyse, waarbij alleen naar OSI-lagen 2 en 3 wordt gekeken, volgens haar eveneens tekort schiet: *“omdat daarmee geen voldoende inzicht wordt verkregen in de vragen die spelen [te weten: welke apps op welke smartphones (met welke besturingssystemen) tot veel signaleringen in het netwerk leiden, toevoeging door het CBP]. (...) Het kan zo zijn dat één server (of straks één cloud cluster) een grote hoeveelheid van applicaties verwerkt. Alleen kijken naar de serverbestemming zegt daarom te weinig over het effect op signalering in het mobiele domein. Uitsplitsing naar het type applicatie in relatie tot het device is belangrijke input.”⁴⁸ En: “De populariteit van applicaties groeit snel, maar wel in onderling sterk verschillende mate. Als alleen de totale networkload in hoeveelheden data als indicatie voor de groei zou worden gebruikt, zou het verschil in netwerk(signalerings-)gebruik niet worden meegenomen. Een adequaat rekenmodel voor het technisch vertalen van het aantal apps naar netwerksignalering bestaat niet en zal lastig zijn te ontwikkelen. (...) Om al deze redenen is het niet (langer) afdoende om de verkeersontwikkeling alleen op de lagen 2 en 3 (de internetlaag, met adressering op basis van IP adressen en de transportlaag, met gebruik van poortnummers), te bewaken.”⁴⁹*

KPN schrijft in haar zienswijze 1 dat de verwerkte gegevens uitsluitend worden gebruikt voor kwantitatief statistisch en technisch onderzoek. Met dit onderzoek wordt beoogd om uitspraken te doen over netwerkbelasting en netwerkgebruik en de verwachte toename daarvan (het betreffen dus trendanalyses).⁵⁰

In haar zienswijze 1 voegt KPN daaraan toe dat de data-analyse volgens KPN noodzakelijkerwijs wordt uitgevoerd op niet-geanonimiseerde data: *“Wanneer het KPN [VERTROUWELIJK] de gegevens direct bij verzameling onomkeerbaar zou anonimiseren, wordt het voor haar onmogelijk om trends op individueel gebruikers niveau te volgen. Dit zou betekenen dat KPN uitsluitend een algemene extrapolatie zou zien van de absolute stijging in bijvoorbeeld algemene signalen. Dit is onvoldoende om voorspellingen te kunnen doen voor benodigde uitbreidingen in het netwerk.*

Bij anonimisering kan bijvoorbeeld niet worden gezien of bepaalde gebruikers meer dan andere gebruikers bijvoorbeeld gebruik maken van bepaalde apps, op basis waarvan voorspellingen kunnen worden gedaan.

Als bijvoorbeeld in bepaalde gebieden veel jonge mensen wonen en ‘early adopters’ zal meer uitbreiding van het netwerk nodig zijn, dan in gebieden waar dit niet het geval is.

⁴⁷ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 5.

⁴⁸ Idem, p. 5-6.

⁴⁹ Idem, p. 3-4.

⁵⁰ Zienswijze 1 KPN, p. 49.

Anonimisering betekent ook dat het onmogelijk wordt om überhaupt dergelijke gebruikersgroepen te identificeren.⁵¹

Het CBP heeft er (weliswaar) kennis van genomen dat er naast het uitbreiden van de (signalerings)capaciteit in het mobiele netwerk ook andere mogelijkheden, en initiatieven bestaan om de druk op het signaleringskanaal te verminderen. Zo hebben volgens berichtgeving in de media grote mobiele aanbieders zoals France Telecom, Deutsche Telekom en Telefónica (Spanje) medio 2011 aangekondigd in overleg te (willen) gaan met makers van besturingssystemen van smartphones en app-ontwikkelaars om de gebruikte software anders in te richten, op een manier die netwerkvriendelijker is.⁵² Ook KPN levert hieraan indirect een bijdrage, via haar apparatuur leverancier [VERTROUWELIJK] die overlegt met app-ontwikkelaars, *"teneinde de belasting van de applicaties waar mogelijk met technische ingrepen in de software te verminderen; bijvoorbeeld door synchronisatie-momenten met het netwerk te randomiseren in plaats van gelijktijdig te laten plaatsvinden, werkzaamheden die door software developers 's nachts in de VS worden uitgevoerd maar hier in piektijden plaatshebben beter te spreiden, etc."*⁵³ De GSM Association, een wereldwijd samenwerkingsverband in de telecomindustrie, heeft in februari 2012 de eerste van een serie activiteiten aangekondigd, bedoeld om netwerkaanbieders te helpen om te gaan met het grotere aantal signaleringen als gevolg van smartphones en apps, te weten: 'Guidelines for Creating More Efficient Mobile Applications' (een developer's guide) en de 'Smarter Apps Challenge' (een competitie om de ontwikkeling van netwerkvriendelijkere apps te stimuleren).⁵⁴ Ter relativering van het belang en de mogelijkheden van zulke initiatieven wijst KPN er in haar zienswijze 2 (evenwel) op dat (i) het langere termijn initiatieven zijn die tot nu toe niet hebben geleid tot concrete oplossingen, (ii) het slagen van zulke samenwerkingsprojecten afhankelijk is van de medewerking van producenten van smartphone besturingssystemen en apps die een tegengesteld belang hebben aan dat van de telecommunicatieaanbieders (een chatty app draagt bij aan de gebruiksbeleving), terwijl (iii) KPN compleet afhankelijk van de goodwill van deze ontwikkelaars - die niet centraal zijn georganiseerd - omdat zij geen enkel juridisch middel heeft om de ontwikkeling van minder netwerk belastende apps af te dwingen.⁵⁵

Het CBP stelt verder vast dat het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, (de gevolgen van) de toename van het datavolume relativeert in de (concept) netneutraliteitsrichtsnoeren, met de volgende zinsneden: *"One should, however, refrain from drawing hasty conclusions from mobile data growth forecasts, which may often be exaggerated and may be compensated for, to a certain extent, by*

⁵¹ Idem, p. 49; zie ook idem, p. 51-53.

⁵² Zie Michelle Donegan, 'Operators Urge Action Against Chatty Apps' (Verslag over de Open Mobile Summit), *Light Reading Mobile* 9 juni 2011. URL: http://www.lightreading.com/document.asp?doc_id=208775 (URL laatst bezocht op 29 mei 2013).

⁵³ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 3.

⁵⁴ GSM Association, 'GSMA Announces New Initiatives Focusing On Creating More Efficient Mobile Applications', 7 februari 2012. URL: <http://www.gsma.com/newsroom/gsma-announces-new-initiatives-focusing-on-creating-more-efficient-mobile-applications/> (URL laatst bezocht op 29 mei 2013).

⁵⁵ Zienswijze 2 KPN, p. 12-13.

*larger customer bases and lowering bandwidth costs. Especially when considering that although the overall data traffic is increasing, the growth rate of traffic is declining over time for fixed and mobile networks. Furthermore, prices for transit and content delivery network services have decreased on a per unit basis as a result of decreases in equipment costs.”*⁵⁶

Volgens KPN slaat de relativering door BEREC echter louter op de toename in dataverkeer (aantallen bytes) en is deze (daarom) niet toepasbaar op de ongekende groei die KPN ervaart in het signaleringsverkeer (aantallen signaleringen) dat over haar mobiele netwerk gaat. KPN erkent dat de groei van dataverkeer, hoewel een uitdaging, van een andere orde is.⁵⁷

KPN benadrukt in haar zienswijze 2 daarnaast, onder verwijzing naar berichtgeving in de media over ernstige verstoringen in het mobiele netwerk van twee andere Europese telecommunicatieaanbieders in verband met signaleringsverkeer, groeiprognozes van [VERTROUWELIJK] (gemiddeld groeipercentage van 252%, verwacht groeipercentage voor Europa van 320% per jaar) en de aandacht in het nieuws die verstoringen in het netwerk van Nederlandse telecommunicatieaanbieders krijgen, dat de impact die het toegenomen signaleringsverkeer wereldwijd heeft op mobiele netwerken van telecommunicatieaanbieders actueel blijft.⁵⁸

Data-analyse apparatuur

KPN gebruikt(e) ten minste twee verschillende soorten data-analyse apparatuur (meetapparaten) voor het doeleinde netwerkplanning en -beheer. Het gaat om de [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] (tot 21 september 2012)⁵⁹ en de [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK].⁶⁰

[VERTROUWELIJK: apparatuur]

KPN is in november 2010 een pilot gestart met de [VERTROUWELIJK: apparatuur]. Uit de contractdocumentatie voorafgaand aan de pilot volgt dat KPN specifiek heeft gekeken of de data-analyse apparatuur rapportages kan uitdraaien met gegevens op abonneeniveau. In de documentatie is in dat verband opgemerkt dat de data-analyse apparatuur in staat moet zijn om: [VERTROUWELIJK].

De [VERTROUWELIJK: apparatuur] is eind 2010 door KPN aangekocht. KPN verklaart daarover: “KPN heeft bij de snelle opkomst van smartphones en applicaties in

⁵⁶ BoR (12) 131. BEREC Guidelines for quality of service in the scope of net neutrality dated 26 November 2012, p. 17. URL: http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/?doc=1101 (URL laatst bezocht op 29 mei 2013). Zie ook BEREC Guidelines for Quality of Service in the scope of Net Neutrality. Draft for public consultation, dated 29 May 2012, p. 17.

⁵⁷ Zienswijze 2 KPN, p. 9.

⁵⁸ Idem, p. 10-12.

⁵⁹ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011. De [VERTROUWELIJK]-apparatuur bevindt zich in Nederland, maar de data-analyse wordt gedaan door [VERTROUWELIJK]. KPN heeft een bewerkersovereenkomst met [VERTROUWELIJK] gesloten. Naleving van het bepaalde in artikel 14 (bewerkersovereenkomst) en 76 (doorgifte van persoonsgegevens naar derde landen) van de Wbp valt buiten de scope van dit onderzoek.

⁶⁰ Reactie KPN op verzoek om inlichtingen van 7 december 2011, p. 2 en reactie KPN op verzoek om inlichtingen van 15 december 2011.

eerste instantie met [VERTROUWELIJK] gesproken welke mogelijkheden er bestonden om goed zicht op de ontwikkelingen te houden (...). [VERTROUWELIJK] bleek daarbij met de [VERTROUWELIJK: apparatuur] over een in andere netwerken beproefd tool te beschikken dat door KPN in eerste instantie in het kader van een pilot is gebruikt. (...) Voor zover KPN bekend is worden vergelijkbare middelen (inmiddels) ook door andere leveranciers geboden. Omdat [VERTROUWELIJK] en de bevindingen in de pilot aan de verwachtingen hebben beantwoord heeft KPN geen verder onderzoek naar technische alternatieven met vergelijkbare functionaliteiten gedaan.”⁶¹

Bezoek aan en gebruik van apps en websites

De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze met behulp van vooraf gedefinieerde en ingestelde filtermodules gegevens verzamelt, vastlegt en bewaart⁶² over het bezoek aan en gebruik van apps en websites, zoals het verbruikte datavolume en de tijdseenheid per app, alsmede het bezoek aan en gebruik van apps per abonnee (de hoeveelheid en categorieën gegevens die nodig zijn om een bepaalde app te identificeren, verschilt per app).⁶³

KPN licht in haar zienswijze 2 toe dat de data-analysetools van KPN waren ingesteld om een beperkt aantal (vooraf gedefinieerde) applicaties te identificeren, waarbij telkens slechts het eerste datapakketje werd geanalyseerd (van een reeks pakketjes die samen een bericht vormen) op grond van vooraf gedefinieerde kenmerken. Hierbij werd enkel gekeken naar verkeersgegevens, zoals protocollen en headers. De communicatie-inhoud was niet van belang om te komen tot een succesvolle identificatie. Ook wanneer de eindgebruiker de inhoud van zijn communicatie zou hebben versleuteld door middel van encryptie (en het derhalve niet mogelijk was om door middel van de data-analysetools de inhoud ‘te lezen’), bleef identificatie van de applicatie mogelijk.⁶⁴

De [VERTROUWELIJK: apparatuur] herkende/identificeerde aldus een (groot) aantal vooraf gedefinieerde apps en websites, zoals [VERTROUWELIJK] (zie **bijlage II**).⁶⁵

⁶¹ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 4-5.

⁶² Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4-5; bijlage 3 bij deze reactie, p. 2-3 en e-mail KPN aan OPTA van 30 mei 2011.

⁶³ Bijlage 3 bij reactie KPN op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1:

“Doel van dit meetapparaat is

- (trend) Analyse van belasting van netwerkelementen*
- Inzage in hoogverbruik (excessief verbruik buiten de voorwaarden – FUP)*
- Inzage in bedreigingen voor mobiele klanten, zoals portscans / virussen)*
- Inzage in welke applicaties / toestelplatformen worden gebruikt in relatie tot signalering belasting.”*

⁶⁴ Zienswijze 2 KPN, p. 7-8.

⁶⁵ Bijlage 4 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, opgenomen als bijlage II bij dit rapport. Bijlage 2 bij reactie KPN op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 2: “Belangrijk is hierbij de definitie van ‘inhoud’. Er zijn twee typen inhoud:

- *de inhoud van een pakketje (m.b.v. een URL);*
- *de inhoud van de boodschap tussen gebruiker en server. (...)*

Om applicaties te kunnen herkennen is een aantal kenmerken hiervan geconfigureerd (denk bv aan de URL van de website van de applicatie zoals bijv. www.facebook.com). Deze URL wordt gekenmerkt met een label voor statische doeleinden in de IP-flow. De inhoud van de communicatie van de gebruiker wordt nooit gebruikt of opgeslagen. De andere analyse van de pakketjes wordt gedaan op de onderliggende lagen (ip adressen van-naar en portnr / protocol)” Bijlage 4 bij reactie

KPN heeft aan een standaardlijst drie apps/services laten toevoegen, namelijk Hyves, WhatsApp en Viber (een app voor VoIP-gesprekken; internettelefonie) (hierna gezamenlijk te noemen: de vooraf gedefinieerde apps en websites).⁶⁶

In haar zienswijze 1 licht KPN haar werkwijze als volgt nader toe. Het KPN [VERTROUWELIJK] paste data-analyse technologieën toe voor het maken van voorspellingen over toename in dataverkeer in het kader van haar netwerkplanning en -beheer. Daartoe moest KPN, zo betoogt zij, zowel kijken naar het signaleringsverkeer dat via het GTP-C kanaal wordt vervoerd als naar het dataverkeer dat via het GTP-U kanaal loopt: op basis van louter het signaleringsverkeer is het volgens KPN niet mogelijk om te onderscheiden op welke soort dataverkeer (bijvoorbeeld welke apps) de signaleringen betrekking hebben (dataverkeer moet worden gecorreleerd met specifieke signaleringen). [VERTROUWELIJK]

Technisch vond de gegevensverwerking door KPN als volgt plaats.

Data- en signaleringsverkeer packets van alle KPN abonnees werden realtime⁶⁷ door/langs een filter met inspectieregels geleid. De gedetecteerde gegevens met betrekking tot het bezoek aan en gebruik van de hierboven genoemde vooraf gedefinieerde apps en websites werden vervolgens per abonnee geordend.⁶⁸ Dit betekent dat: (i) wanneer een abonnee geen van de vooraf vastgestelde apps op zijn smartphone had staan en gebruikte, de [VERTROUWELIJK: apparatuur] van deze abonnee in het geheel geen gegevens over zijn gebruik verzamelde en opsloeg; (ii) wanneer een abonnee wel een vooraf vastgestelde app op zijn smartphone had staan en gebruikte, de [VERTROUWELIJK: apparatuur] alleen die gegevens verzamelde en bewaarde die nodig waren om de app te kunnen identificeren (de hoeveelheid en categorieën gegevens die nodig zijn om een bepaalde app te identificeren, verschilt per app).⁶⁹

KPN licht in haar zienswijze 1 nader toe dat de data-analyse apparatuur die KPN inzette telkens uitsluitend de (header) informatie inspecteerde [VERTROUWELIJK] dat naar de applicatieserver gaat: *“Wat er terugkomt aan informatie vanaf de server wordt niet bekeken (hierin zit de inhoud van een webpagina bijvoorbeeld).”*⁷⁰ KPN merkt daarbij op: *“de data-analyse technieken die KPN toepast, inspecteren verder niet alle eerste pakketjes die over het GTP-U kanaal worden vervoerd. KPN selecteert alleen die apps die naar verwachting het meeste signaleringsverkeer veroorzaken (...) Door slechts de vooraf bepaalde applicaties te correleren met de*

KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1: *“The [VERTROUWELIJK: apparatuur] identifies applications based on a combination of server IP addresses, ports, protocols, HTTP hosts, HTTP URIs, HTTP referrers [VERTROUWELIJK: (...)].”*

⁶⁶ Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 5.

⁶⁷ Bijlage 5 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011.

⁶⁸ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5; reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 5 en bijlage 3 bij deze reactie, p. 4. E-mail KPN aan OPTA van 30 mei 2011.

⁶⁹ Zienswijze 2 KPN, p. 7-8.

⁷⁰ Zienswijze 1 KPN, p. 43-44.

bijbehorende signaleringen, verwerkt KPN op het GTP-C kanaal ook slechts die signaleringen die verband houden met de internetssessie van deze applicaties.”⁷¹

KPN verzamelde⁷² (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement (afhankelijk van de apps die zij op hun smartphones hadden staan) enerzijds het MSISDN (06-nummer)⁷³, het IMSI-nummer (uniek klantnummer)⁷⁴ en het IMEI-nummer (uniek toestelnummer)⁷⁵ en anderzijds de hostname (URL op hoofddomein), de referer (laatst bezochte URL) of (bij bijvoorbeeld Hyves) het IP-adres van-naar met poortnummer/gebruikt protocol⁷⁶, [VERTROUWELIJK], evenals aantallen bytes/packets (volume), frequentie (het aantal keren dat verbinding wordt gemaakt), starttijd en eindtijd sessie [VERTROUWELIJK].⁷⁷

Ten aanzien van de app herkenning verklaart KPN: *"Volgens de opgave van de leverancier kijkt de [VERTROUWELIJK: apparatuur] op meerdere lagen naar de IP pakketjes om vast te stellen welke applicatie wordt gebruikt. Daarbij wordt onder meer naar de URL gekeken. (...) Om applicaties te kunnen herkennen is een aantal kenmerken hiervan geconfigureerd (denk bv aan de URL van de website van de applicatie zoals bijv. www.facebook.com). (...) De andere analyse van de pakketjes wordt gedaan op de onderliggende lagen (ip adressen van-naar en poortnr/protocol)."*⁷⁸ KPN voegt daaraan toe dat met de [VERTROUWELIJK: apparatuur] onderzoek werd gedaan naar de meest belastende applicaties en waarom ze zo belastend zijn.⁷⁹

Vervolgens werden deze gegevens per abonnee opgeslagen [VERTROUWELIJK] in de achterliggende database⁸⁰ en gedurende een periode van negentig dagen bewaard.⁸¹

⁷¹ Idem, p. 46.

⁷² Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3, 5 en 6; e-mail KPN aan OPTA van 30 mei 2011 en bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011.

⁷³ Idem, p. 5.

⁷⁴ Het IMSI-nummer is opgeslagen op de SIM-kaart. Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5; reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 5 en bijlage 3 bij deze reactie, p. 4; e-mail KPN aan OPTA van 30 mei 2011.

⁷⁵ Het IMEI-nummer is opgeslagen in de mobiele telefoon. E-mail KPN aan OPTA van 30 mei 2011.

⁷⁶ Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 5; e-mail KPN aan OPTA van 30 mei 2011.

⁷⁷ E-mail KPN aan OPTA van 30 mei 2011. Bijlage 1 van de bewerkersovereenkomst tussen KPN B.V. en [VERTROUWELIJK: (...)] van 3 november 2010.

⁷⁸ Bijlage 3 - De inzet van de [VERTROUWELIJK: apparatuur] bij brief KPN aan het Landelijk Parket van 25 mei 2011, p. 2. Bijlage 1 bij reactie KPN op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 3: *Bij patroonherkenning wordt er binnen de applicatie laag [VERTROUWELIJK: (...)] gezocht op herkenningstekens. (...) "/mobiel/opwaarderen-en-beltegoed/Online-opwaarderen.htm" een identifier die gebruikt kan worden om de dienst 'prepaid opwaarderen' te herkennen. (...) Bij gedragherkenning wordt er naar het gedrag van het protocol gekeken, bijv. pakketgrootte, het aantal data pakketten per flow etc. (...) Bij statistische analyse, vaak gebruikt in combinatie met gedragherkenning, wordt afgeleid aan bijv. spreiding van pakketgrootte gedurende bepaalde tijd."* Zie ook reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 4.

⁷⁹ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 3.

⁸⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5 en e-mail KPN aan OPTA van 30 mei 2011.

Via een gebruikersinterface konden (afhankelijk van de apps die zij op hun smartphones hadden staan) per abonnee (of op een geaggregeerd niveau) onder andere de volgende gegevens worden geraadpleegd: enerzijds het MSISDN⁸², het unieke IMSI-klantnummer⁸³ en het unieke IMEI-toestelnummer en anderzijds (de netwerkbelasting door) het bezoek aan en gebruik van de vooraf gedefinieerde apps en websites onderscheidenlijk gebruikte toestel(len), onderverdeeld naar verbruikte datavolume (aantallen bytes/packets)⁸⁴, *airtime* (tijdsvenster)⁸⁵ en signaleringen (frequentie; het aantal keren dat verbinding wordt gemaakt) [VERTROUWELIJK].⁸⁶

AFBEELDING II: Voorbeeld schermafdruck user interface [VERTROUWELIJK: apparatuur]⁸⁷

[VERTROUWELIJK]

Ten slotte draaide KPN vanaf november 2010⁸⁸ (voor wat betreft WhatsApp: sinds februari 2011⁸⁹) tot september 2012 rapportages uit op abonneeniveau met deze gegevens.⁹⁰ Deze rapportages bevatten (afhankelijk van de apps die zij op hun smartphones hadden staan) onder andere het MSISDN⁹¹, het unieke IMSI-klantnummer⁹² en (de netwerkbelasting door) het bezoek aan en gebruik van de vooraf gedefinieerde apps en websites onderverdeeld naar verbruikte datavolume (aantallen bytes/packets) en signaleringen (frequentie).

In **bijlage III** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde netwerkplanning en -beheer verwerkte gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

[VERTROUWELIJK: apparatuur]

Daarnaast maakt KPN gebruik van de [VERTROUWELIJK: apparatuur] om ten aanzien van het inkomende en uitgaande data roaming verkeer fouten in signaleringen te lokaliseren zodat deze kunnen worden hersteld en om de prestaties van het netwerk te bewaken (performance indicatoren etc.).⁹³ De inzet van data-analyse technieken valt buiten de scope van dit onderzoek voor zover het betrekking heeft op data roaming verkeer.

(Algemene) technische en organisatorische maatregelen

KPN verklaart in reactie op een verzoek om inlichtingen van OPTA een combinatie

⁸¹ Idem, p. 6; idem.

⁸² Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5.

⁸³ KPN [VERTROUWELIJK: apparatuur] Pilot van 9 september 2010, p. 13.

⁸⁴ Idem.

⁸⁵ Idem.

⁸⁶ Bijlage 1 van de bewerkersovereenkomst tussen KPN B.V. en [VERTROUWELIJK: (...)] van 3 november 2010.

⁸⁷ [VERTROUWELIJK: (...)] Datasheet, p. 1.

⁸⁸ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 3.

⁸⁹ Idem.

⁹⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5.

⁹¹ Idem.

⁹² Idem.

⁹³ Reactie KPN op verzoek om inlichtingen van 15 december 2011, p. 1.

van technische en organisatorische maatregelen te hanteren, waaronder de KPN Security Policy onder andere gebaseerd op de ISO27001 standaard voor beveiligingsbeheer, toegangsautorisaties (slechts een beperkte groep medewerkers heeft toegang tot de server waarover het dataverkeer wordt afgewikkeld), toegangsbeveiliging door middel van [VERTROUWELIJK].⁹⁴

Informatie voor abonnees

Het algemene Privacy Statement van KPN (versie januari 2011) (hierna: het oude Privacy Statement) bevatte de volgende informatie over de verwerking van gegevens ten behoeve van netwerkplanning en -beheer, voor zover voor dit onderzoek van belang:

“In dit privacy statement hebben wij nader voor je op een rij gezet hoe wij omgaan met je persoonsgegevens. (...) Als je gebruik maakt van je vaste- of mobiele telefoonaansluiting of gebruik maakt van internet dan ‘vervoeren’ wij gegevens van je. Deze gegevens worden ook wel aangeduid als verkeersgegevens. Het gaat dan om gegevens zoals het tijdstip en de duur van het gebruik van een aansluiting, het opgeroepen nummer, surfgedrag op internet en je IP-adres. KPN slaat de gegevens over het gebruik van je vaste- of mobiele aansluiting op. Je surfgedrag wordt niet opgeslagen. KPN houdt niet bij welke websites je bezoekt. (...) KPN neemt geen kennis van de inhoud van je e-mailberichten. KPN neemt evenmin kennis van de inhoud van je chatberichten. (...) Als je gebruik maakt van een locatiegebonden dienst, zoals mobiele telefonie of zgn. nomadische VOIP diensten, dan verwerken wij je locatiegegevens (de plaats waar gebruik wordt gemaakt van de mobiele of nomadische aansluiting)”, (onderstreping toegevoegd door het CBP).⁹⁵

Verder bevatte de privacyverklaring van Hi (hierna: de oude privacyverklaring) de volgende informatie:

“Hi heeft de doelen waarvoor wij gegevens verwerken gebundeld in één document, het “privacy statement” van Hi. (...) Wij verwerken persoonsgegevens (zoals naam, adres, woonplaats, e-mailadres, telefoonnummer, afgenomen diensten en factuurgegevens op hoofdlijnen) voor de volgende doeleinden: (...)”

⁹⁴ Reactie KPN op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 5-7. Naleving van het bepaalde in artikel 13 (beveiliging) van de Wbp valt buiten de scope van dit onderzoek.

⁹⁵ Privacy Statement Januari 2011. URL: <http://www.kpn.com/privacy.htm> (webpagina toegankelijk tot mei 2012). Vgl. ook Algemene Voorwaarden voor mobiele telecommunicatiediensten (versies januari 2007, juli 2009 en januari 2011): “KPN kan de in het eerste lid bedoelde gegevens verwerken voor commerciële, ideële en charitatieve doeleinden, waaronder marktonderzoek, marketing- en verkoopactiviteiten, beoordeling van kredietwaardigheid, bestrijding van fraude en verstrekking aan derden, met inachtneming van de voor de desbetreffende verwerking geldende doeleinden en mogelijkheden tot verzet, zoals nader aangeduid in het Privacystatement.” Zie in dezelfde zin de Algemene Voorwaarden voor mobiele telecommunicatiediensten (Hi versies december 2007, juli 2009 en januari 2011) en de Algemene en Aanvullende Voorwaarden Hi (versie maart 2012). URL: <http://www.hi.nl/Overig/Algemene-voorwaarden.htm> (URL laatst bezocht op 29 mei 2013).

e. Netwerkmanagement, waaronder netwerkplanning en netwerkachitectuur en fraudedetectie (...)

Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...)

b. Ten behoeve van verkeersbeheer", (onderstreping toegevoegd door het CBP).⁹⁶

Het CBP stelt vast dat er in de privacyverklaring/algemene voorwaarden geen (andere) informatie werd gegeven over de categorieën van verwerkte gegevens, en de bewaartermijn.

KPN geeft in haar zienswijze 1 aan dat het algemene KPN privacy statement ongelukkig was geformuleerd, bijvoorbeeld waar de verkeersgegevens die KPN verwerkte (onder meer de URL van de applicatieserver) werden aangeduid met 'surfgedrag'.⁹⁷ KPN verklaart verder dat zij in het licht van de geconstateerde onduidelijkheden en de publieke commotie die is ontstaan rondom de toepassing van data-analyse technieken de KPN en de Hi privacy statements op een aantal punten heeft aangevuld en verduidelijkt.⁹⁸ KPN heeft het CBP op 4 juni 2012 haar nieuwe privacy statements en (kopieën van haar) gewijzigde meldingen verstrekt.

De 'Algemene Voorwaarden voor mobiele telecommunicatiediensten' (versie 30 juli 2012) bepalen:

*"KPN spant zich in om de dienstverlening zo ongestoord mogelijk te laten verlopen. Het is technisch echter onmogelijk om elke storing of beperking van de dienstverlening te voorkomen. Aansprakelijkheid voor het niet of niet goed functioneren van de dienstverlening bestaat alleen binnen de grenzen van deze Algemene Voorwaarden, of voor zover KPN en de Contractant hierover expliciete afspraken in een nadere overeenkomst hebben gemaakt."*⁹⁹

Het nieuwe algemene Privacy Statement van KPN (versie mei 2012) (hierna: het nieuwe Privacy Statement) bepaalt, voor zover voor dit onderzoek van belang:

"Voor de planning en beheer van ons netwerk (...) zetten wij data-analyse technieken in die verkeersgegevens verzamelen en analyseren voor het beheer en de planning van ons netwerk. Wij kijken uitdrukkelijk niet naar de inhoud van de berichten die je stuurt of naar de inhoud van de websites die je bezoekt. Hierna volgt

⁹⁶ Privacy - Hi. URL: <http://www.hi.nl/Overig/Privacy.htm> (webpagina toegankelijk tot mei 2012).

⁹⁷ Zienswijze 1 KPN, p. 72.

⁹⁸ Idem, p. 73.

⁹⁹ Algemene Voorwaarden voor mobiele telecommunicatiediensten (versies januari 2007, juli 2009 en januari 2011). Vgl. ook General Terms and Conditions Mobile Telecommunications Services 2009. Zie in dezelfde zin de Algemene voorwaarden voor mobiele telecommunicatiediensten (Hi versies december 2007, juli 2009 en januari 2011) en de Algemene en aanvullende voorwaarden Hi (versie maart 2012).

een nadere omschrijving van de doeleinden waarvoor wij data-analyse technieken inzetten.

Netwerkplanning en -beheer

KPN is verantwoordelijk voor het telecommunicatienetwerk waarover het telefoon-, data-, of televisieverkeer plaatsvindt. Wij dragen zorg voor het onderhouden, plannen en verbeteren van het netwerk en het beheer zoals het routeren van verkeer, oplossen van storingen, bewaken van piek- en overbelasting. Door het netwerkgebruik te analyseren krijgen wij essentiële informatie over het gebruik en de belasting van ons netwerk. Op basis van deze informatie kunnen wij ons netwerk gericht uitbreiden en verbeteren. Het gaat ons hierbij niet om de inhoud van je communicatie.

KPN verwerkt verkeersgegevens voor deze technische en statistische analyses. Denk hierbij aan (i) telefoniegegevens, waaronder je telefoonnummer, datum en tijdstip van aanvang en einde verbinding, het soort dienst, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI) en (ii) datagegevens, waaronder gebruikersidentificatie, de applicatieserver waarmee apps die jij gebruikt verbinding maken, datum en tijdstip van de log-in en log-off van een internetdienst, e-maildienst of internettelefoniedienst of IP-adres. De uitkomsten van deze analyses worden geanonimiseerd gerapporteerd binnen KPN en zijn niet langer herleidbaar tot individuen. (...)

KPN bewaart je gegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de verwerking van de doeleinden waarvoor je gegevens worden verwerkt. Hoe lang bepaalde gegevens worden bewaard is afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per doel verschillen.

Als je een abonnement bij KPN hebt dan worden je gegevens in ieder geval tenminste gedurende de looptijd van je abonnement bewaard. In het kader van de Wet bewaarplicht bewaren wij je verkeersgegevens gedurende zes maanden”, (onderstreping toegevoegd door het CBP).¹⁰⁰

De nieuwe privacyverklaring van Hi bevat soortgelijke informatie. Verder bevat de nieuwe privacyverklaring van Hi de volgende informatie:

*“Wij verwerken persoonsgegevens voor de volgende doeleinden:
(...) e. Netwerkmanagement, waaronder netwerk- en verkeersbeheer, netwerkplanning en netwerkarchitectuur, fraudedetectie en bevordering van netwerkintegriteit en –continuïteit (zoals het beveiligen van het Hi netwerk tegen veiligheidsinbreuken, spam en malware); (...)*

*Wij verwerken je verkeersgegevens voor de volgende doeleinden:
(...) b. Ten behoeve van netwerkmanagement, waaronder netwerk- en verkeersbeheer, netwerkplanning en netwerkarchitectuur, fraudedetectie en*

¹⁰⁰ Bijlage XI bij brief KPN van 4 juni 2012. URL: <http://www.kpn.com/privacy.htm>. Naleving van het bepaalde in artikel 10 van de Wbp (bewaartermijn) valt buiten de scope van dit onderzoek.

*bevordering van netwerkindegriteit en –continuïteit (zoals het beveiligen van het Hi netwerk tegen veiligheidsinbreuken, spam en malware); (...)*¹⁰¹

Getroffen maatregelen: stopzetten [VERTROUWELIJK: apparatuur] en anonimiseringsoplossing

KPN heeft besloten de [VERTROUWELIJK: apparatuur] met ingang van 21 september 2012 stop te zetten en gestopt te houden. KPN geeft verder (onderbouwd met een verklaring¹⁰²) aan alle via de [VERTROUWELIJK: apparatuur] opgeslagen data én de geanonimiseerde [VERTROUWELIJK: apparatuur]-data die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening, te hebben verwijderd per uiterlijk 11 oktober 2012. KPN is daarnaast in overleg getreden met de leverancier van de [VERTROUWELIJK: apparatuur] over een technisch alternatief dat ervoor zorgt dat verkeersgegevens zo snel mogelijk omkeerbaar worden geanonimiseerd. KPN acht zo'n alternatief proportioneel.¹⁰³

KPN heeft het CBP nadere inlichtingen verstrekt omtrent de door [VERTROUWELIJK] geoffreerde en door KPN voorgestelde anonimiseringsoplossing voor de [VERTROUWELIJK: apparatuur] die KPN voornemens is te implementeren, waarin (samengevat weergegeven) [VERTROUWELIJK] om op een minst ingrijpende manier voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer te kunnen komen tot statistisch betrouwbare analyses van trends in haar mobiele netwerk. KPN heeft daarbij toegezegd (aanvullende) technische en organisatorische waarborgen te treffen om de risico's op heridentificatie te minimaliseren en doelbinding te garanderen (waaronder [VERTROUWELIJK]).¹⁰⁴ [VERTROUWELIJK] De totale ontwikkel- en licentiekosten van de [VERTROUWELIJK: apparatuur] zijn in de periode tot 30 juni 2013 in totaal [VERTROUWELIJK].¹⁰⁵ KPN heeft aangegeven dat de nieuwe anonimiseringsoplossing naar verwachting 1 juni 2013 in gebruik wordt genomen.

2.5 Prepaid- en MMS-verkeer

Als tweede verzamel- en verwerkingsdoeleinde van gegevens noemt KPN de facturering van MMS- en prepaidverkeer. KPN verklaart: *“Teneinde bepaalde verkeersstromen buiten databundels te kunnen factureren worden bepaalde URL's herkend. Het gaat daarbij tot op heden uitsluitend om MMS verkeer (...) en verkeer van prepaidklanten naar een opwaardeersite (...).”*¹⁰⁶

Data-analyse apparatuur

KPN gebruikt vanaf 2002-2003 data-analyse apparatuur [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] in haar mobiele netwerk ten behoeve van het faciliteren van het bezoek aan en gebruik van

¹⁰¹ Bijlage XII bij brief KPN van 4 juni 2012. URL: <http://www.hi.nl/Overig/Privacy.htm> (URL laatst bezocht op 29 mei 2013).

¹⁰² Bijlage 1 bij reactie KPN op vordering van 28 februari 2013.

¹⁰³ Zienswijze 2 KPN, p. 2-5.

¹⁰⁴ Reactie KPN verzoek om inlichtingen van 6 en 15 februari 2013. Reactie KPN op vordering van 28 februari 2013.

¹⁰⁵ Reactie KPN op verzoek om inlichtingen van 15 februari 2013, p. 11-12.

¹⁰⁶ Reactie KPN verzoek om inlichtingen van 1 september 2011, p. 1.

(gratis) opwaardeersites bij een ontoereikend prepaid tegoed en de facturering van MMS-verkeer.¹⁰⁷

KPN verklaart dat voor dit doeleinde alleen realtime naar informatie wordt ‘gekeken’, om prepaid- en MMS-verkeer te herkennen. Er vindt geen opslag plaats van gegevens over het dataverkeer.¹⁰⁸

KPN verklaart dat data-analyse technieken niet ‘conditioneel’ (dat wil zeggen: alleen als een prepaid klant geen tegoed meer heeft) kunnen worden toegepast.¹⁰⁹

Technisch vond de gegevensverwerking door KPN als volgt plaats.

Prepaidverkeer

Een prepaid abonnee betaalt vooraf voor het gebruik van datadiensten. KPN houdt het tegoed van de prepaid abonnee bij in een factureringssysteem [VERTROUWELIJK]. Als een prepaid abonnee een datasessie wil starten, herkent de [VERTROUWELIJK: apparatuur] deze abonnee als prepaid abonnee. Voordat een verbinding wordt opgebouwd, vraagt de [VERTROUWELIJK: apparatuur] aan het factureringssysteem of de prepaid abonnee nog voldoende tegoed heeft. Als het tegoed van de abonnee ontoereikend is, geeft het factureringssysteem geen toestemming voor een verbinding en zal de datasessie niet slagen. Er was (tot stopzetting van de data-analysefunctionaliteit op de [VERTROUWELIJK: apparatuur] op 3 oktober 2012) dan alleen bezoek en gebruik mogelijk van gratis opwaardeersites (URL's) totdat het tegoed was opgewaardeerd.¹¹⁰

Bij een gratis URL vroeg de [VERTROUWELIJK: apparatuur] niet aan het factureringssysteem of de abonnee nog voldoende tegoed had. Om gratis URL's te herkennen werden data-analyse technieken toegepast.

KPN licht in haar zienswijze 1 toe dat de [VERTROUWELIJK: apparatuur] naar de URL van de website [VERTROUWELIJK] ‘keek’. Wanneer het een URL betrof van een gratis opwaardeersite, verleende de [VERTROUWELIJK: apparatuur] de prepaid abonnee toegang.¹¹¹

In **bijlage III** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde prepaidverkeer verwerkte gegevens.

MMS-verkeer

MMS (*Multimedia Messaging Service*) is de multimediale opvolger van SMS.

Dataverkeer wordt gewoonlijk gefactureerd op basis van de hoeveelheid verkeer gemeten op de APN. Dit is de naam (URL) van het toegangspunt tot internet

¹⁰⁷ Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1-2.

¹⁰⁸ Reactie KPN verzoek om inlichtingen van 1 september 2011, p. 6. Bijlage 2 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1; e-mail KPN aan OPTA van 30 mei 2011.

¹⁰⁹ E-mail KPN aan OPTA van 30 mei 2011.

¹¹⁰ Bijlage 2 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

¹¹¹ Zienswijze 1 KPN, p. 63.

(bijvoorbeeld iphonekpn.nl). Voor MMS-verkeer geldt een vast tarief per bericht. Om dubbele facturering van MMS-verkeer te voorkomen wordt binnen de volumemeting van dataverkeer het MMS gerelateerde volume als gratis aangemerkt. Om dit MMS-verkeer te herkennen worden data-analyse technieken toegepast.¹¹²

KPN licht in haar zienswijze 1 toe dat het netwerksysteem van KPN MMS standaard als 'normaal dataverkeer' beschouwt. Om dat te voorkomen analyseert KPN met de [VERTROUWELIJK: apparatuur] op basis van de URL van de MMS-Centrale of het dataverkeer een MMS betreft [VERTROUWELIJK]. Als het een MMS is, wordt het volume van de MMS afgetrokken van het totale dataverbruik binnen de databundel.¹¹³

De inzet van data-analyse technieken valt buiten de scope van dit onderzoek voor zover het de facturering van MMS-verkeer betreft.

Informatie voor abonnees

Het oude Privacy Statement van KPN bevatte de volgende informatie over de verwerking van gegevens ten behoeve van de facturering van MMS-verkeer en het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed, voor zover voor dit onderzoek van belang:

*"KPN verwerkt je persoons-, verkeers- en locatiegegevens in de eerste plaats om onze diensten aan je te kunnen leveren. Voor het in behandeling nemen van aanvragen, het tot stand brengen van een aansluiting, het opbouwen van verbindingen, het versturen van een (al dan niet gespecificeerde) nota, notanavraag en het afhandelen van storingsmeldingen of klachten, is verwerking van je gegevens noodzakelijk."*¹¹⁴

Verder bevatte de oude privacyverklaring van Hi de volgende informatie:

"Wij verwerken persoonsgegevens (zoals naam, adres, woonplaats, e-mailadres, telefoonnummer, afgenomen diensten en factuurgegevens op hoofdlijnen) voor de volgende doeleinden: (...)

d. Het factureringsproces, waaronder het opstellen en afdrukken van een nota, incasso, fraudepreventie en fraudeonderzoek, expensive call monitoring, interconnectie-betalingen. (...)

Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...)

*a. Ten behoeve van het vervaardigen van nota's"*¹¹⁵

¹¹² Bijlage 2 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011. Het is niet onwaarschijnlijk dat de MMS-dienst, gelet op het gebruik dat daarvan in het algemeen wordt gemaakt, van steeds minder groot belang wordt/is.

¹¹³ Zienswijze 1 KPN, p. 62.

¹¹⁴ Privacy Statement Januari 2011.

¹¹⁵ Privacy - Hi.

De ‘Algemene Voorwaarden voor mobiele telecommunicatiediensten’ bepalen:

“KPN biedt de Contractant van een Prepaid-aansluiting één of meer mogelijkheden om Prepaid-tegoed op te waarderen. KPN kan de bedragen vaststellen waarmee Prepaid-tegoed kan worden opgewaardeerd en kan de hoogte van deze bedragen wijzigen. Voor specifieke Diensten kan KPN separate vormen van Prepaid-tegoed hanteren. (...)

*(...) KPN zal het relevante Prepaid-tegoed bij gebruik van de Prepaid-aansluiting afwaarderen met de verschuldigde vergoedingen. Als het Prepaid-tegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante Dienst te gebruiken en kan het gebruik van de Prepaid-aansluiting worden verbroken”, (onderstreping toegevoegd door het CBP).*¹¹⁶

Het CBP stelt vast dat er in de privacyverklaring/algemene voorwaarden geen (andere) informatie werd gegeven over de categorieën van verwerkte gegevens, en de bewaartermijn.

Het nieuwe algemene Privacy Statement van KPN bepaalt, voor zover voor dit onderzoek van belang:

“Voor (...) facturering van prepaidklanten en MMS-verkeer, zetten wij data-analyse technieken in die verkeersgegevens verzamelen en analyseren voor het beheer en de planning van ons netwerk. Wij kijken uitdrukkelijk niet naar de inhoud van de berichten die je stuurt of naar de inhoud van de websites die je bezoekt. (...)

Facturering van prepaidklanten en MMS-verkeer
Daarnaast zetten wij data-analysetechnieken in voor facturering van prepaid- en MMS-verkeer. Wanneer je een prepaidklant bent, sturen wij je geen nota, omdat je verbruikte kosten meteen op je tegoed in mindering worden gebracht. KPN houdt daarom je tegoed bij en kan er zo voor zorgen dat prepaidklanten zonder voldoende beltegoed toegang hebben tot opwaardeerwebsites met hun toestel.

*Wanneer je een MMS-bericht verstuurt, wordt aan de hand van het URL-adres van de MMS-server vastgesteld waar het bericht naartoe wordt gestuurd om te kunnen bepalen dat het om een MMS-bericht gaat. Hierdoor kunnen wij ervoor zorgen dat een MMS-bericht niet dubbel wordt gefactureerd (namelijk als MMS-bericht en als data via je databundel.*¹¹⁷

De nieuwe privacyverklaring van Hi bevat soortgelijke informatie. Verder bevat de nieuwe privacyverklaring van Hi de volgende informatie:

¹¹⁶ Vgl. ook Algemene Voorwaarden voor mobiele telecommunicatiediensten (versies januari 2007, juli 2009, januari 2011). Zie in dezelfde zin de Algemene voorwaarden voor mobiele telecommunicatiediensten (Hi versies december 2007, juli 2009 en januari 2011) en de Algemene en aanvullende voorwaarden Hi (versie maart 2012).

¹¹⁷ Bijlage XI bij brief KPN van 4 juni 2012.

*“Wij verwerken persoonsgegevens voor de volgende doeleinden:
 (...) d. Het factureringsproces inclusief facturering van prepaid en MMS-diensten, waaronder het opstellen en afdrukken van een nota, incasso, fraudepreventie en fraudeonderzoek, expensive call monitoring, interconnectie-betalingen; (...) Wij verwerken je verkeersgegevens voor de volgende doeleinden:
 (...) a. Ten behoeve van het factureringsproces inclusief facturering van prepaid en MMS-diensten, waaronder het opstellen en afdrukken van een nota, incasso, fraudepreventie en fraudeonderzoek, expensive call monitoring, interconnectie-betalingen; (...)”¹¹⁸*

Getroffen maatregelen: stopzetten ‘data-analysefunctionaliteit’

KPN heeft besloten de ‘data-analysefunctionaliteit’ van de [VERTROUWELIJK: apparatuur] met ingang van 3 oktober 2012 stop te zetten en gestopt te houden. Als alternatief voor de data-analyse functionaliteit van de [VERTROUWELIJK: apparatuur] verleent KPN thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK], op zo’n manier dat [VERTROUWELIJK]. KPN licht nader toe dat KPN nu toegang verleent tot gratis opwaardeersites op basis [VERTROUWELIJK]. Hiermee verloopt het faciliteren van toegang tot (gratis) opwaardeersites via [VERTROUWELIJK].¹¹⁹

2.6 Firewalls, spamfilters en virusscanners

Als derde verzamel- en verwerkingsdoeleinde van gegevens noemt KPN het gebruik van firewalls, spamfilters en virusscanners. KPN verklaart dat de inzet van data-analyse technieken voor dit doeleinde noodzakelijk is: *“Firewalls worden in het netwerk toegepast om het netwerk te beschermen tegen aanvallen op de netwerkelementen. (...) Wanneer er grote hoeveelheden spam of malware (de verzamelnaam voor alle vormen van kwaadaardige software) vanuit een netwerk wordt verstuurd neemt binnen de internetgemeenschap de reputatie van dit netwerk af. Andere Service Providers zullen op basis van het bronadres delen van dit netwerk gaan blokkeren om zo hun eigen klanten te beschermen. Dit kan resulteren in een degradatie in de internetdienstverlening; sites zullen voor KPN klanten niet meer te bereiken zijn en mail vanuit het mobiele KPN domein zal door andere providers worden geweigerd.”¹²⁰*

KPN gebruikt vanaf 2000 data-analyse apparatuur (thans: firewalls van de [VERTROUWELIJK] leveranciers [VERTROUWELIJK] en een anti-spam oplossing tegen virussen en spam van de [VERTROUWELIJK] leverancier [VERTROUWELIJK].¹²¹

¹¹⁸ Bijlage XII bij brief KPN van 4 juni 2012.

¹¹⁹ Idem, p. 74-75.

¹²⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 4-5.

¹²¹ Idem, p. 2. Reactie KPN op verzoek om inlichtingen van 7 december 2011, p. 2.

KPN inspecteert en analyseert het dataverkeer¹²² van al haar abonnees met een (prepaid of postpaid) data abonnement en zorgt ervoor dat spam en malware/virussen tegen worden gehouden en verwijderd.¹²³

Het is (ook) volgens het CBP algemeen aanvaard dat het voor mobiele aanbieders bij spamfiltering en virus- en malwarebestrijding niet volstaat om alleen naar headergegevens te kijken. Ten aanzien van spamfiltering geldt dat de meeste mobiele aanbieders ook naar de inhoud van e-mails moeten kijken (naar de data inhoud van packets), om spam te kunnen herkennen. Dat gebeurt bijvoorbeeld aan de hand van veelgebruikte woorden, zoals 'Viagra'. Bij de bestrijding van virussen en malware worden over het algemeen lijsten gebruikt met de 'fingerprints' (vooraf gedefinieerde herkenningsspatronen), die worden opgesteld door gespecialiseerde security-bedrijven. Om nieuwe, nog niet-geïnterpreteerde virussen en malware te kunnen herkennen, zijn heuristische (zelflerende) technieken nodig die eveneens inhoudelijk kijken in bestanden naar kwaadaardige code.¹²⁴

In **bijlage III** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde het gebruik van firewalls, spamfilters en virusscanners verwerkte gegevens.

Informatie voor abonnees

De oude privacyverklaring van Hi bevatte de volgende informatie over de verwerking van gegevens ten behoeve van netwerkintegriteit en -continuïteit, voor zover voor dit onderzoek van belang:

"Wij verwerken persoonsgegevens (zoals naam, adres, woonplaats, e-mailadres, telefoonnummer, afgenomen diensten en factuurgegevens op hoofdlijnen) voor de volgende doeleinden: (...)

f. Ten behoeve van een verantwoorde bedrijfsvoering, waaronder beveiliging, risicobeperking, integriteitsonderzoek, behandeling van ongewenste oproepen, uitbreiding en verbetering van dienstverlening. (...)

Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...)

*b. Ten behoeve van verkeersbeheer"*¹²⁵

De 'Aanvullende Voorwaarden voor gebruik van het mobiel netwerk van KPN voor datadiensten' bevatten de volgende informatie over de verwerking van gegevens ten behoeve van firewalls, spamfilters en virusscanners:

¹²² Daaronder begrepen inhoud van door abonnees (gedownload) bestanden en verzonden en ontvangen e-mails aan de hand vooraf gedefinieerde spam-, virus- en malwareherkenningsspatronen, voor zover nodig om spam/virussen/malware tegen te houden en te verwijderen (oftewel, spam-, virus- en malwareherkenningsspatronen uit de inhoud van het dataverkeer).

¹²³ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 2.

¹²⁴ Een toelichting op virusbestrijdingstechnieken is te lezen op URL: http://en.wikipedia.org/wiki/Antivirus_software.

¹²⁵ Privacy - Hi.

*“KPN behoudt zich het recht voor om alle maatregelen te nemen die zij noodzakelijk acht in het belang van de veiligheid en integriteit van haar (vaste en mobiele) netwerk en apparatuur van gebruikers op haar netwerk. Zo kunt u bijvoorbeeld onbedoeld de veiligheid en integriteit van het mobiele netwerk of van mobiele telefoons of computers van derden in gevaar brengen doordat u virussen verspreidt via uw mobiele telefoon of doordat uw mobiele telefoon door een virus onderdeel is geworden van een botnet. (...) KPN zet zich in om verspreiding van ongevraagde e-mail (spam) gericht aan haar gebruikers te beperken. Voor zover nodig geeft u toestemming aan KPN om spam te verwijderen of het vervoer ervan via haar netwerk te blokkeren”, (onderstreping toegevoegd door het CBP).*¹²⁶

Het CBP stelt vast dat er in de privacyverklaring/algemene voorwaarden geen (andere) informatie werd gegeven over de categorieën van verwerkte gegevens, en de bewaartermijn.

Het nieuwe algemene Privacy Statement van KPN bepaalt, voor zover voor dit onderzoek van belang:

“Voor (...) de beveiliging van ons netwerk (...) zetten wij data-analyse technieken in die verkeersgegevens verzamelen en analyseren voor het beheer en de planning van ons netwerk. (...)

Beveiliging van ons netwerk en jouw aansluiting

KPN draagt zorg voor beveiliging van ons netwerk en jouw aansluiting daarop. Zo maken we gebruik van geavanceerde technieken (zoals firewalls, spamfilters en virusscanners) voor de bescherming tegen veiligheidsinbreuken, virussen, spam en malware. Voor meer informatie over hoe jij zelf je verbinding kan beveiligen, klik hier.

*Om jouw aansluiting en ons netwerk tegen veiligheidsinbreuken, virussen, spam en malware te beschermen, wordt al het bel- en internetverkeer dat ons netwerk binnenkomt en verlaat automatisch gescand door deze beveiligingstechnieken. Wanneer wij constateren dat een bericht bijvoorbeeld een virus bevat dan zullen wij proberen dit virus te verwijderen en het bericht alsnog af te leveren tenzij dit spam betreft.”*¹²⁷

De nieuwe privacyverklaring van Hi bevat soortgelijke informatie. Verder bevat de nieuwe privacyverklaring van Hi de volgende informatie:

*“Wij verwerken persoonsgegevens voor de volgende doeleinden:
(...) e. Netwerkmanagement, waaronder netwerk- en verkeersbeheer,
netwerkplanning en netwerkarchitectuur, fraudedetectie en bevordering van*

¹²⁶ Aanvullende Voorwaarden voor gebruik van het mobiel netwerk van KPN voor datadiensten (geldig vanaf 5 september 2011). URL: <http://www.kpn.com/allevoorwaarden/algemene-voorwaarden-mobiel/Mobiele-Telecom-diensten.htm>.

¹²⁷ Bijlage XI bij brief KPN van 4 juni 2012.

netwerkindegriteit en -continuïteit (zoals het beveiligen van het Hi netwerk tegen veiligheidsinbreuken, spam en malware); (...)

Wij verwerken je verkeersgegevens voor de volgende doeleinden:

*(...) b. Ten behoeve van netwerkmanagement, waaronder netwerk- en verkeersbeheer, netwerkplanning en netwerkarchitectuur, fraudedetectie en bevordering van netwerkindegriteit en -continuïteit (zoals het beveiligen van het Hi netwerk tegen veiligheidsinbreuken, spam en malware); (...)*¹²⁸

2.7 Behandeling van klantklachten

Ten slotte noemt KPN als verzamel- en verwerkingsdoeleinde van gegevens de behandeling van klantklachten. KPN verklaart dat het hierbij (in tegenstelling tot de overige drie verzameldoeleinden) gaat om concrete, individuele klantklachten.¹²⁹ KPN verklaart dat de inzet van data-analyse technieken in deze gevallen noodzakelijk is *“om te kijken waarom bepaalde routeringen niet goed functioneren. Daarvoor kan het kijken in meerdere lagen nodig zijn en soms kan het zelfs noodzakelijk zijn de inhoud daarin mee te nemen.”*¹³⁰

KPN gebruikt vanaf 2000 data-analyse technieken [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] in het kader van de afhandeling van klantklachten.¹³¹

KPN verklaart voor de behandeling van klantklachten veelal realtime mee te ‘kijken’ met het dataverkeer van de betreffende KPN-abonnees over haar mobiele netwerk.¹³² De gegevens over en uit het dataverkeer worden alleen opgeslagen als ook offline analyse noodzakelijk is.¹³³

KPN verklaart dat deze verwerking is gebaseerd op toestemming: *“Voor zover het voor de behandeling van de klantklacht noodzakelijk is om de inhoud van het dataverkeer te openen dan wordt de klant hier vooraf op gewezen en wordt aan de klant uitdrukkelijk toestemming hiervoor gevraagd.”*¹³⁴

In **bijlage III** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde behandeling van klantklachten verwerkte gegevens.

Informatie voor abonnees

Het oude Privacy Statement van KPN bevatte de volgende informatie over de verwerking van gegevens ten behoeve van de behandeling van klantklachten, voor zover voor dit onderzoek van belang:

¹²⁸ Bijlage XII bij brief KPN van 4 juni 2012.

¹²⁹ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 4.

¹³⁰ Idem, p. 2.

¹³¹ Idem. Bijlage 2 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

¹³² E-mail 30 mei 2011 van KPN aan OPTA.

¹³³ Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

¹³⁴ Idem. Reactie KPN op verzoek om inlichtingen van 7 december 2011, p. 2.

“KPN verwerkt je persoons-, verkeers- en locatiegegevens in de eerste plaats om onze diensten aan je te kunnen leveren. Voor het in behandeling nemen van aanvragen, het tot stand brengen van een aansluiting, het opbouwen van verbindingen, het versturen van een (al dan niet gespecificeerde) nota, notanavraag en het afhandelen van storingsmeldingen of klachten, is verwerking van je gegevens noodzakelijk”, (onderstreping toegevoegd door het CBP).¹³⁵

Verder bevatte de oude privacyverklaring van Hi de volgende informatie:

“Wij verwerken persoonsgegevens (zoals naam, adres, woonplaats, e-mailadres, telefoonnummer, afgenomen diensten en factuurgegevens op hoofdlijnen) voor de volgende doeleinden: (...)

c. Het beheer van de relatie tussen jou en Hi, waaronder alle activiteiten in verband met de voorbereiding en de uitvoering van de met jou gesloten overeenkomst, zoals nota aanvraag, klachtafhandeling, storingsopheffing en advisering. (...)

Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...)

c. Ten behoeve van de afhandeling van verzoeken om inlichtingen van je met betrekking tot je eigen aansluiting”¹³⁶

Het CBP stelt vast dat er in de privacyverklaring/algemene voorwaarden geen (andere) informatie werd gegeven over de categorieën van verwerkte gegevens, en de bewaartermijn.

De nieuwe privacyverklaring van Hi bevat de volgende informatie:

“Wij verwerken persoonsgegevens voor de volgende doeleinden:

(...) c. Het beheer van de relatie tussen jou en Hi, waaronder alle activiteiten in verband met de voorbereiding en de uitvoering van de met jou gesloten overeenkomst, zoals nota aanvraag, klachtafhandeling, storingsopheffing en advisering; (...)

Wij verwerken je verkeersgegevens voor de volgende doeleinden:

(...) c. Ten behoeve van de afhandeling van verzoeken om inlichtingen van je met betrekking tot je eigen aansluiting; (...)¹³⁷

Nieuw(e) systeem/[VERTROUWELIJK: apparatuur]-omgeving om klantklachten over te hoge rekeningen op te kunnen lossen

KPN heeft in het kader van de nadere inlichtingen omtrent de door [VERTROUWELIJK] geoffreerde en door KPN voorgestelde anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) die KPN voornemens is te implementeren aangegeven voornemens te zijn (ook) een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-

¹³⁵ Privacy Statement Januari 2011.

¹³⁶ Privacy - Hi.

¹³⁷ Bijlage XII bij brief KPN van 4 juni 2012.

omgeving in te richten om - ondanks de anonimiseringsoplossing - klantklachten over te hoge rekeningen op te kunnen (gaan) lossen.¹³⁸

De (mogelijke) toekomstige inzet van data-analyse technieken voor de behandeling van klantklachten via een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-omgeving valt buiten de scope van dit onderzoek.

2.8 Verdere verwerking

KPN verstrekke vanaf februari 2011 tot september 2012 rapportages uit de [VERTROUWELIJK: apparatuur] aan het KPN retailbedrijf ten behoeve van marktonderzoek (analyse van de eigen dienstverlening).¹³⁹

KPN verklaart dat *“de resultaten van de specifieke analyse op het gebruik van applicaties (...) uiteraard tevens van belang [zijn, toevoeging door het CBP] voor de retailafdeling van KPN. (...) De retailafdeling van KPN wordt namelijk sinds enige tijd geconfronteerd met een omzetsdaling als gevolg van een daling van het SMS verkeer, mogelijk als gevolg van de toename van applicaties. De uitkomsten van de door de [VERTROUWELIJK: apparatuur] uitgevoerde analyse kunnen helpen deze omzetsdaling te verklaren. (...) De retailafdeling heeft deze geaggregeerde gegevens geanalyseerd om de geconstateerde daling in het SMS verkeer te verklaren en zich te oriënteren op de mogelijkheden om nieuwe proposities in de markt te zetten.”*¹⁴⁰

KPN heeft in april 2011 de volgende (per abonnee geaggregeerde) gegevens over het gebruik van WhatsApp door haar abonnees (over de periode februari-april 2011¹⁴¹) uit de [VERTROUWELIJK: apparatuur] aan het KPN retailbedrijf verstrekt¹⁴²: het aantal dagen waarop WhatsApp is gebruikt, de eerste en de laatste dag waarop WhatsApp is gebruikt en het totale aantal bytes dat met WhatsApp is uitgewisseld (in combinatie met de unieke IMSI-klantnummers).¹⁴³ Het KPN retailbedrijf heeft vervolgens uit deze set, op grond van de IMSI-nummers, de gegevens van de Hi abonnees gehaald voor nadere analyse.¹⁴⁴

KPN verklaart in haar zienswijze 1 dat de [VERTROUWELIJK] van de [VERTROUWELIJK] die beschikking had over de gegevens, het IMSI-nummer heeft gebruikt om gebruik van WhatsApp, leeftijdsgroep etc. af te kunnen leiden, zodat gebruiksgroepen konden worden onderscheiden.¹⁴⁵

¹³⁸ Zie o.a. reactie KPN op vordering van 28 februari 2013, p. 1.

¹³⁹ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4 en reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 5-6.

¹⁴⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3 en 6. Zie ook reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4: *“Het toegenomen gebruik van WhatsApp in combinatie met de al eerder waargenomen daling in het gebruik van SMS, heeft er toe geleid dat KPN zich op dit moment oriënteert op de mogelijkheden om nieuwe proposities in de markt te zetten.”*

¹⁴¹ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

¹⁴² Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3 en bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

¹⁴³ Idem, p. 3.

¹⁴⁴ Idem. Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

¹⁴⁵ Zienswijze 1 KPN, p. 69.

KPN verklaart dat het haar uit marktonderzoek bekend is dat Hi abonnees als eerste plegen over te stappen op nieuwe toepassingen en diensten en dat de analyse door het KPN retailbedrijf zich daarom op die klantgroep heeft geconcentreerd.¹⁴⁶ KPN verklaart dat de gegevens na de analyse door het KPN retailbedrijf zijn geanonimiseerd.¹⁴⁷ Dit is gedaan door de laatste vier cijfers van de IMSI-nummers te vervangen door een X.¹⁴⁸

Het KPN retailbedrijf wilde vooral inzicht hebben/krijgen in het gebruik van WhatsApp door Hi abonnees (als 'early adopters').¹⁴⁹

KPN verklaart in haar zienswijze 1 hierover: *"De verstrekking aan de afdeling [VERTROUWELIJK] was niet in overeenstemming met [VERTROUWELIJK]. Zodra het management van KPN kennis kreeg van dit incident is het incident onderzocht, is de analyse direct stopgezet en zijn nadere organisatorische maatregelen genomen om herhaling te voorkomen. De betrokken personen bij het incident zijn allen specifiek hierop aangesproken."*¹⁵⁰

KPN heeft ook na april 2011 gegevens uit de [VERTROUWELIJK: apparatuur] verstrekt aan het KPN retailbedrijf voor marktonderzoek. Van 29 juli 2011 tot september 2012 heeft zij periodiek gegevens verstrekt uit de [VERTROUWELIJK: apparatuur] (afhankelijk van de apps die zij op hun smartphones hadden staan) over het gebruik van een (groot) aantal apps en websites door al haar abonnees met een (prepaid of postpaid) data abonnement. KPN verklaart dat dit sinds 29 juli 2011 alleen in geanonimiseerde vorm gebeurde.¹⁵¹ KPN verklaart dat de gegevens volledig en onomkeerbaar waren geanonimiseerd omdat voorafgaand aan de verstrekking aan het KPN retailbedrijf de unieke IMSI-klantnummers waren verwijderd en de bestanden ook geen andere unieke nummers bevatten.¹⁵²

Informatie voor abonnees

Het oude Privacy Statement van KPN bevatte de volgende informatie over de verwerking van gegevens ten behoeve van marktonderzoek- en marketingdoeleinden:

"KPN verwerkt je persoonsgegevens ten behoeve van marktonderzoek en marketing- en verkoopactiviteiten (ook na beëindiging van het contract) ten behoeve van eigen dienstverlening van KPN en aan KPN gelieerde ondernemingen. Je gegevens worden verwerkt voor het doen van (gezamenlijke) aanbiedingen, zowel schriftelijk, telefonisch als elektronisch (onder meer via SMS en e-mail). Ook je verkeersgegevens kunnen door KPN gebruikt worden voor marketingdoeleinden en voor het doen van aanbiedingen, maar uitsluitend voor zover je daarvoor vooraf je

¹⁴⁶ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3.

¹⁴⁷ E-mail KPN aan OPTA van 30 mei 2011 en bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

¹⁴⁸ Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4 en e-mail KPN aan OPTA van 30 mei 2011.

¹⁴⁹ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3. Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

¹⁵⁰ Zienswijze 1 KPN, p. 69.

¹⁵¹ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3.

¹⁵² Idem.

toestemming hebt gegeven. Je verkeersgegevens worden niet verwerkt voor het doen van aanbiedingen van derden en worden ook niet aan derden verstrekt”,
(onderstreping toegevoegd door het CBP).¹⁵³

Verder bevatte de oude privacyverklaring van Hi de volgende informatie:

“Wij verwerken persoonsgegevens (zoals naam, adres, woonplaats, e-mailadres, telefoonnummer, afgenomen diensten en factuurgegevens op hoofdlijnen) voor de volgende doeleinden: (...)

i. Het doen van marktonderzoek en marketing- en verkoopactiviteiten (ook na beëindiging van het contract) ten behoeve van de dienstverlening en de verkoop van producten en diensten van Hi. (...)

Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...)

f. Ten behoeve van marktonderzoek en verkoopactiviteiten voor producten en diensten van Hi, ook na beëindiging van het contract, mits je daarvoor toestemming hebt gegeven”.¹⁵⁴

Het CBP stelt vast dat er in de privacyverklaring/algemene voorwaarden geen (andere) informatie werd gegeven over de categorieën van verwerkte gegevens, en de bewaartermijn.

Het nieuwe algemene Privacy Statement van KPN bevat de volgende aanvullende informatie:

“Trendanalyse

KPN voert onderzoek uit naar trends in de markt door middel van statistische analyses. Voorzover verkeersgegevens nodig zijn voor deze trendanalyses, maakt KPN uitsluitend gebruik van geanonimiseerde verkeersgegevens. De informatie die wij uit deze analyses halen, gebruiken wij om onze huidige producten- en dienstenportfolio en processen te evalueren en deze aan te passen op grond van nieuwe ontwikkelingen. Deze onderzoeksresultaten worden niet gebruikt voor specifiek op jou gerichte marketing- en verkoopactiviteiten. (...)

Marketing- en verkoopactiviteiten

KPN verwerkt je persoonsgegevens (niet zijnde verkeersgegevens) ten behoeve van marketing- en verkoopactiviteiten (ook na beëindiging van het contract) ten behoeve van eigen dienstverlening van KPN. Je gegevens worden verwerkt voor het doen van (gezamenlijke) aanbiedingen, zowel schriftelijk, telefonisch als elektronisch (onder meer via SMS en e-mail).

Uitsluitend indien je daarmee hebt ingestemd worden ook je verkeersgegevens door KPN gebruikt voor marketing- en verkoopactiviteiten en voor het doen van

¹⁵³ KPN Privacy Statement Januari 2011.

¹⁵⁴ Privacy - Hi.

aanbiedingen. Je verkeersgegevens worden niet verwerkt voor het doen van aanbiedingen van derden en worden ook niet aan derden verstrekt."¹⁵⁵

De nieuwe privacyverklaring van Hi bevat soortgelijke informatie.¹⁵⁶

Getroffen maatregelen: stopzetten [VERTROUWELIJK: apparatuur] en verwijdering gegevens

KPN heeft besloten de [VERTROUWELIJK: apparatuur] met ingang van 21 september 2012 stop te zetten en gestopt te houden, behoudens nader tegenbericht. KPN geeft verder (onderbouwd met een verklaring¹⁵⁷) aan alle via de [VERTROUWELIJK: apparatuur] opgeslagen data én de geanonimiseerde [VERTROUWELIJK: apparatuur]-data die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening, te hebben verwijderd per uiterlijk 11 oktober 2012.

¹⁵⁵ Bijlage XI bij brief KPN van 4 juni 2012.

¹⁵⁶ Bijlage XII bij brief KPN van 4 juni 2012.

¹⁵⁷ Bijlage 1 bij reactie KPN op vordering van 28 februari 2013.

3. UITWERKING VAN HET WETTELIJK KADER EN BEOORDELING

3.1 Wettelijk kader: samenloop Wbp en Tw

Op de verwerking van persoonsgegevens in de sector elektronische communicatie (telecommunicatiesector) is de algemene privacyrichtlijn 95/46/EG (hierna: Privacyrichtlijn) van toepassing (geïmplementeerd in de Wbp).¹⁵⁸ De Privacyrichtlijn regelt de verwerking van persoonsgegevens en de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, waaronder het recht op (bescherming van de) persoonlijke levenssfeer. Daarnaast gelden de bepalingen uit de richtlijn betreffende privacy en elektronische communicatie 2002/58/EG (e-Privacyrichtlijn) (geïmplementeerd in de Tw).¹⁵⁹ De e-Privacyrichtlijn regelt de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor gebruikers van openbare elektronische communicatiediensten.¹⁶⁰ De bepalingen uit de e-Privacyrichtlijn geven aan bepaalde algemene normen uit de algemene Privacyrichtlijn een nadere invulling (bijvoorbeeld een nadere begrenzing/inperking van de toegestane verwerkingen).¹⁶¹ Er is geen sprake van een *lex specialis*-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene.¹⁶² Wel geldt dat indien en voor zover de e-Privacyrichtlijn (als geïmplementeerd in de Tw) ten aanzien van de verwerking van persoonsgegevens op een bepaald punt een uitputtende regeling bevat, die regeling voorgaat op de algemene normen uit de Privacyrichtlijn (als geïmplementeerd in de Wbp).¹⁶³

In de wetsgeschiedenis is daarover het volgende opgemerkt:

“In zijn algemeenheid kan niet worden gesteld dat bijzondere wetgeving voor de meer algemene privacyvoorschriften gaat. Dit adagium [te weten: de regel ‘lex specialis derogat legi generali’; toevoeging door het CBP] gaat alleen op in die gevallen dat de bijzondere wet ten opzichte van de Wbp een exclusieve werking heeft, dat wil zeggen een uitputtende regeling bevat waarnaast de Wbp geen gelding meer heeft. Een opsomming van dergelijke specifieke wetgeving staat in artikel 2

¹⁵⁸ “Onder het bereik van de algemene privacyrichtlijn, en in het verlengde daarvan de Wbp, valt iedere verwerking van persoonsgegevens waarover enige feitelijke macht kan worden uitgeoefend”, *Kamerstukken II 1997/98, 25 533, nr. 5, p. 115.*

¹⁵⁹ Zie artikel 1, tweede lid, van de e-Privacyrichtlijn; zie ook overweging 12 van de e-Privacyrichtlijn.

¹⁶⁰ Zie artikel 1, eerste lid, van de e-Privacyrichtlijn; zie ook overwegingen 4, 8 en 12 van de e-Privacyrichtlijn.

¹⁶¹ Zie artikel 1, tweede lid, en overweging 12 van de e-Privacyrichtlijn. Zie ook *Kamerstukken II 2002/03, 28 851, nr. 7, p. 53, Kamerstukken II 1997/98, 25 533, nr. 5, p. 114-115 en Kamerstukken I 1997/98, 25 533, nr. 309d, p. 8. Kamerstukken II 2002/03, 28 851, nr. 3, p. 59: “Voor zover verkeersgegevens zijn aan te merken als persoonsgegevens, dat wil zeggen: gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, geeft hoofdstuk 11 van de wet, in het bijzonder artikel 11.5, in aanvulling op (in het bijzonder) de algemene voorwaarden die op grond van hoofdstuk 2, paragraaf 1, van de Wbp aan de verwerking van persoonsgegevens worden gesteld, nadere - uitputtende - voorschriften.”*

¹⁶² Zie overweging 10 van de e-Privacyrichtlijn: “In de sector elektronische communicatie is Richtlijn 95/46/EG van toepassing, met name op alle aangelegenheden met betrekking tot de bescherming van fundamentele rechten en vrijheden die niet specifiek onder het bepaalde in deze richtlijn vallen, met inbegrip van de plichten van de verantwoordelijke en de rechten van personen”, (onderstreping toegevoegd door het CBP).

¹⁶³ Zie ook *Kamerstukken II 2002/03, 28 851, nr. 3, p. 45.*

van de Wbp. In de gevallen dat de specifieke wetgeving niet valt onder het bereik van dit artikel 2, geldt de regel «bijzondere wet gaat voor algemene wet» echter niet. De Wbp geldt in deze gevallen immers naast de specifieke wetgeving. Alsdan heeft de Wbp dus een aanvullende werking, namelijk voor die onderdelen die niet door de bijzondere wetgeving worden gedekt. De Organisatiewet sociale verzekeringen 1997 en de Telecommunicatiewet zijn daar een voorbeeld van. De geheimhoudingsvoorschriften in de Organisatiewet sociale verzekeringen vormen dus een uitwerking van die in de Wbp. Wel is het zo dat de voorschriften van de Wbp daarmee niet als direct bindende normen in beeld komen, ze spelen enkel zijdelings een rol.”¹⁶⁴

De toepasselijkheid van de Wbp op de verwerking van persoonsgegevens in de sector elektronische communicatie is niet uitgesloten in de Wbp, of in de Tw. Integendeel. Artikel 11.2 van de Tw bepaalt bijvoorbeeld: *“Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of krachtens deze wet bepaalde dragen de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, onderscheidenlijk zijn dienst”, (onderstreping toegevoegd door het CBP).*

¹⁶⁴ Kamerstukken II 1999/2000, 26 410, nr. 7, p. 2. Zie in dezelfde zin Kamerstukken II 1997/98, 25 892, nr. 3, p. 177: *“In § 4 van het Algemeen deel van de toelichting «Algemene normen en sectorale invulling» noemden wij twee modellen van aanvullende wetten: het eerste waarbij uitputtend de gegevensbescherming in een wet is geregeld en het tweede waarbij in aanvulling op de Wet bescherming persoonsgegevens nadere regels zijn gesteld. Wordt het eerste model gevolgd, dan wordt de toepasselijkheid van het onderhavige wetsvoorstel uitdrukkelijk uitgesloten. (...) Wordt het tweede model gevolgd, dan is de Registratiekamer op grond van het wetsvoorstel bevoegd.”* Vgl. ook Kamerstukken II 1997/98, 25 892, nr. 3, p. 13: *“Voor het overige zullen veel bijzondere wetten op onderdelen concretisering bevatten, gericht op de sector die zij regelen. Het gaat daarbij formeel om leges speciales die derogeren aan de bepalingen van dit wetsvoorstel, maar materieel om een sectorale invulling die moet worden beoordeeld tegen de achtergrond van deze algemene normen, mede gelet op het feit ook deze bijzondere wetten aan de richtlijn [95/46/EG, toevoeging door het CBP] zullen moeten voldoen voor zover zij geheel of ten dele communautair recht bestrijken. (...) In artikel 2 WPR is ervan uitgegaan dat bij wetten van het tweede model [te weten: een uitputtend, bijzonder (privacy-)regime, waarbij in de wet wordt vermeld dat de toepasselijkheid van de algemene regels geheel wordt uitgesloten] de niet-toepasbaarheid van WPR steeds in deze laatste wet zelf is vastgelegd. Het onderhavige wetsvoorstel kiest voor een continuering van dit systeem. Deze keuze brengt met zich dat ook bij eventuele toekomstige wetgeving bevattende een uitputtend regime voor de bescherming van persoonsgegevens in een bepaalde sector, het niet van toepassing zijn van de WBP in deze laatste wet zelf wordt vermeld. Deze keuze voorkomt vragen over de verhouding tussen verschillende wettelijke systemen”, (onderstreping toegevoegd door het CBP).*

3.2 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*.¹⁶⁵

KPN, gevestigd en kantoorhoudende te Den Haag, Nederland, bepaalt de doeleinden van en de middelen voor de verwerking van persoonsgegevens bij de inzet van data-analyse technieken op het dataverkeer over haar mobiele netwerk.¹⁶⁶ KPN heeft zich, voor zover voor dit onderzoek van belang, op 3 september 2010 als verantwoordelijke gemeld bij het CBP. Uit de gegevens uit het Handelsregister volgt dat KPN bevoegd is om doel en middelen vast te stellen. KPN is daarmee de verantwoordelijke voor deze verwerking in de zin van artikel 1, aanhef en onder d, van de Wbp.

3.3 Verwerking van 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.¹⁶⁷

Uitwerking van het wettelijk kader

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

“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.”

¹⁶⁵ Overweging 47 van de Privacyrichtlijn luidt in dit verband: “Overwegende dat, wanneer een bericht dat persoonsgegevens bevat, wordt verzonden via een telecommunicatie- of elektronische postdienst waarvan het enige doel is dit soort berichten door te geven, het de persoon is van wie het bericht uitgaat, en niet degene die de dienst aanbiedt, die normaliter zal worden beschouwd als verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk voor de verwerking van de aanvullende persoonsgegevens die noodzakelijk zijn voor de werking van de dienst.”

¹⁶⁶ Zie ook URL: <http://www.kpn.com/Privacy.htm>.

¹⁶⁷ 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”.

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 (...).”

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd.¹⁶⁸

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking¹⁶⁹ hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of - gezien de context¹⁷⁰ waarin ze worden verwerkt - medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.¹⁷¹ 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 een persoonsgegeven.¹⁷² 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.¹⁷³ Als voorbeeld wordt in de wetsgeschiedenis bij de Wbp genoemd het telefoonnummer.¹⁷⁴

¹⁶⁸ Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.

¹⁶⁹ Zie WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 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.

¹⁷⁰ Vgl. idem, p. 11: 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.

¹⁷¹ 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.

¹⁷² Idem. Zie ook 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”.

¹⁷³ Idem, p. 46-47.

¹⁷⁴ Idem: “Tevens dienen telefoonnummers (Registratiekamer 8 juli 1993, 93.A.002) (...) onder omstandigheden als een persoonsgegeven te worden aangemerkt.” En Kamerstukken II 1998/99, 25 892, nr. 6, p. 27: “Telefoonnummers zijn niet altijd persoonsgegevens in de zin van de wet, bijvoorbeeld niet wanneer deze zijn toegekend aan een rechtspersoon of een bestuursorgaan en het

Volgens de wetsgeschiedenis zijn “gegevens van een netwerkbeheerder over het gebruik van het netwerk via aansluitpunten teneinde het goed functioneren van het netwerk te waarborgen, (...) geen persoonsgegevens zolang elke reële mogelijkheid is uitgesloten dat die gegevens worden gebezigd om het gebruik van het netwerk door individuele personen in ogenschouw te nemen.”¹⁷⁵

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 persoon¹⁷⁶ - redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.¹⁷⁷ 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.¹⁷⁸ Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke.¹⁷⁹ In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.¹⁸⁰

Beoordeling

Het CBP heeft in de paragrafen 2.4 tot en met 2.7 (p. 21 e.v. van dit rapport) vastgesteld dat KPN in verschillende apparatuur en systemen (onder andere afhankelijk van de apps die zij op hun smartphones hadden staan) combinaties van de gegevens over en uit het dataverkeer van abonnees van haar dataverkeersdiensten (betrokkenen) verwerkt(e) als beschreven in **bijlage III** bij dit rapport.

nummer niet herleidbaar is tot een individuele natuurlijke persoon, bijvoorbeeld omdat deze een vaste gebruiker is.” 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.” Zie ook Rb. Dordrecht 31 augustus 2004, NBSTRAF 2004, 422 over het GSM-nummer (MSISDN) als persoonsgegeven.

¹⁷⁵ Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

¹⁷⁶ 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.

¹⁷⁷ Idem, 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.

¹⁷⁸ Idem, p. 48. Vergelijk ook WP29 136, p. 16. 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.

¹⁷⁹ Idem, p. 48-49.

¹⁸⁰ Idem, p. 49. Registratiekamer 27 maart 1995, 95.V.029.

Daarbij beschikt KPN over de NAW-gegevens en/of e-mailadressen van (een groot deel van) haar abonnees (zie ook p. 19 van dit rapport), op grond van hun contractuele relatie.

Het CBP heeft in de paragrafen 2.4 tot en met 2.7 (p. 21 e.v. van dit rapport) vastgesteld dat KPN de hierboven genoemde gegevens over en uit het dataverkeer verzamelt, gebruikt (en voor de doeleinden netwerkplanning en -beheer tot 21 september 2012 en voor de behandeling van klantklachten, als ook offline analyse noodzakelijk is, ook: vastlegde/vastlegt en bewaarde/bewaart op individueel persoonsniveau, althans geaggregeerd per abonnee). Dit deed/doet zij om het data ge-/verbruik en netwerkgebruik van betrokkenen in kaart te brengen.

Gegevens 'betreffende' een persoon

Het MSISDN, het unieke IMSI-klantnummer en het IMEI-toestelnummer (unieke klant- en/of toestel identifier(s)), op zichzelf of in onderlinge combinatie of in samenhang met (technische) gegevens over het bezoek aan en gebruik van apps en websites zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over zijn mobiele data ge-/verbruik).¹⁸¹ Datzelfde geldt voor de combinatie met locatiegegevens (Cell ID), die een beeld kunnen geven van de verplaatsingen van de betrokkene, met tijd.

Daarnaast zijn unieke klant- en/of toestel identifier(s), in combinatie met (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene gegevens over een natuurlijke persoon. KPN 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 analyseren van de inhoud van (gedownload) bestanden en verzonden en ontvangen e-mails op spam-, virus- en malware-herkenningspatronen om spam/virussen/malware tegen te houden en te verwijderen, het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed of aan het analyseren van het dataverkeer (inclusief, als dat noodzakelijk is, de inhoud van het dataverkeer) om een verzoek om inlichtingen af te handelen (oftewel, het gebruik van de gegevens in individuele gevallen met betrekking tot abonnees om technische defecten of fouten in de overbrenging van communicatie op te sporen en te verhelpen). De gegevens worden dus door KPN gebruikt op een wijze die in het maatschappelijk verkeer de betrokkene raakt.

Verder kan het mobiele data ge-/verbruik 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.¹⁸²

¹⁸¹ Hieruit volgt informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie.

¹⁸² Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010, p. 35 (z2010-00582). URL: http://www.cbppweb.nl/Pages/pv_20110913_google.aspx (URL laatst bezocht op 29 mei 2013).

Niet doorslaggevend is of KPN de bedoeling heeft om de gegevens over en uit het dataverkeer of voor die doeleinden of andere doeleinden te gebruiken. Er is al sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel kan worden gebruikt¹⁸³, en die mogelijkheid is/was aanwezig. KPN beschikt(e), zoals aangegeven, bijvoorbeeld over informatie over het mobiele datagebruik van individuele betrokkenen (het bezoek aan en gebruik van apps en websites, frequentie en duur/tijd), data verbruiksgegevens (volume) en contactgegevens (waaronder het MSISDN (unieke klantidentificatie), e-mailadres(sen) en/of NAW-gegevens).

In haar zienswijze 1 brengt KPN naar voren dat nu door KPN een strikte scheiding is aangebracht tussen het KPN [VERTROUWELIJK], en de door KPN verwerkte verkeersgegevens niet voor marketingdoeleinden kunnen en worden gebruikt, deze verkeersgegevens geen persoonsgegevens betreffen.¹⁸⁴ [VERTROUWELIJK] KPN benadrukt dat [VERTROUWELIJK].¹⁸⁵

Zoals vermeld, is niet het criterium of KPN de bedoeling heeft om de gegevens over en uit het dataverkeer of voor dat doeleinde of andere doeleinden te gebruiken, maar of de gegevens daarvoor kunnen worden gebruikt. In de wetsgeschiedenis bij de Wbp is in dat verband opgemerkt: *“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.”*¹⁸⁶ Het gebruik voor een op de persoon gericht doel is/was mogelijk. [VERTROUWELIJK].¹⁸⁷

Identificeerbaarheid van de persoon

De gegevens over en uit het dataverkeer zijn op zichzelf, in onderlinge combinatie of in samenhang met uit andere bron bekende informatie voor KPN direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).

Postpaid abonnees

Ten aanzien van KPN abonnees met een postpaid data abonnement, geldt het volgende.

Het MSISDN, het unieke IMSI-klantnummer¹⁸⁸ en het unieke IMEI-toestelnummer van een abonnee met een postpaid data abonnement zijn voor KPN identificerend omdat zij een koppeling(smogelijkheid) heeft tussen deze nummers, gecombineerd met

¹⁸³ Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

¹⁸⁴ Zienswijze 1 KPN, p. 12.

¹⁸⁵ Idem, p. 68 en bijlage VIII bij deze zienswijze.

¹⁸⁶ Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

¹⁸⁷ KPN heeft dit in haar zienswijze erkend. Zienswijze 1 KPN, p. 69.

¹⁸⁸ Aan dit IMSI zijn alle gegevens van een abonnee gebonden, zoals NAW-gegevens, of de abonnee prepaid of een abonnement heeft en of deze wel of niet in het buitenland mag bellen.

NAW-gegevens en/of e-mailadres(sen). Er kan dus een relatie tussen de gegevens worden gelegd.

KPN beschikt(e) verder over een koppeling(smogelijkheid) tussen de unieke klant-en/of toestel identifier(s) en (tot de verwijdering daarvan per uiterlijk 11 oktober 2012) (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps en websites dan wel (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene.¹⁸⁹

Niet alleen beschikt(e) KPN over de (in)direct identificerende gegevens over en uit het dataverkeer in haar databases/bestanden, ook heeft zij ter zake kundige technici in dienst (waaronder de eerder genoemde medewerkers, zie p. 31 van dit rapport) en beschikt zij over de benodigde technische faciliteiten (waaronder applicaties om de databases te bevragen en de technische mogelijkheid om gegevens te exporteren uit deze databases) om de gegevens aan elkaar te koppelen of zo nodig via tussenstappen te herleiden naar de betrokken abonnee. Hieruit blijkt dat de inspanning die KPN moet verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is.

Het CBP neemt verder in aanmerking dat de verwerking van de gegevens volgens KPN voor de volgende doeleinden geschiedt:

- (i) netwerkplanning en -beheer (daaronder mede begrepen het voorkomen van congestie) om op abonneeniveau inzicht te hebben/krijgen in de ontwikkelingen van verkeer, netwerkgebruik etc. in verband met de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps, en in hoogverbruik (excessief verbruik buiten de voorwaarden van de Fair Use Policy; FUP);¹⁹⁰
- (ii) het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed;
- (iii) spamfiltering en virus- en malwarebestrijding in individuele gevallen; en
- (iv) het oplossen van technische incidenten, en klantproblemen in individuele gevallen (behandeling van klantklachten).¹⁹¹

Gegevensverwerkingen voor deze doeleinden hebben slechts nut als die het mogelijk maken specifieke personen te identificeren.

In de opinie van de Artikel 29-werkgroep, het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders, over het begrip persoonsgegevens is in dat verband opgemerkt: *“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*

¹⁸⁹ Ook hier kan een relatie tussen de gegevens worden gelegd.

¹⁹⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 1. Zie ook zienswijze KPN 1 van 24 februari 2012, p. 51. Of KPN een grondslag heeft voor de inzet van data-analyse technieken ten behoeve van (handhaving van) de FUP wordt/is niet door het CBP beoordeeld.

¹⁹¹ Idem, p. 2.

informatie moet dan ook worden beschouwd als informatie betreffende identificeerbare personen, wat betekent dat voor de verwerking de regels inzake gegevensbescherming gelden.”¹⁹² Dit is volgens de opinie van de Artikel 29-werkgroep met name relevant voor statistische informatie, wanneer de informatie weliswaar wordt gepresenteerd als geaggregeerde gegevens, maar (de) andere gegevens identificatie van betrokkenen mogelijk maken.¹⁹³

Om de hiervoor genoemde doeleinden (i) tot en met (iv) te verwezenlijken moe(s)ten 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.

Prepaid abonnees

Ten aanzien van KPN abonnees met een prepaid data abonnement, geldt het volgende.

KPN heeft verklaard dat zij NAW-gegevens en/of e-mailadressen heeft van [VERTROUWELIJK] van de IOM (Internet Op Je Mobiel) en van [VERTROUWELIJK] van de IOL (Internet Op Je Laptop) abonnees met een prepaid data abonnement.¹⁹⁴

Ten aanzien van de prepaid abonnees van wie KPN NAW-gegevens en/of e-mailadressen heeft, beschikt(e) KPN over een koppeling(smogelijkheid) tussen enerzijds de unieke klant- en/of toestel identifier(s), gecombineerd met NAW-gegevens en/of e-mailadressen en anderzijds respectievelijk (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps en websites (tot de verwijdering daarvan per uiterlijk 11 oktober 2012) en gegevens over (het functioneren van het netwerk/toestel bij) het gebruik van het netwerk door een individuele betrokkene. Er kan/kon een relatie tussen de gegevens worden gelegd.

In de wetsgeschiedenis bij de Tw wordt over de identificeerbaarheid van prepaid abonnees opgemerkt: *“Niettemin beschikken aanbieders in veel gevallen - bijvoorbeeld naar aanleiding van acties waarbij prepaid bellers een bepaald gratis beltegoed kunnen verkrijgen waarbij de verstrekking van persoonsgegevens als vereiste is gesteld - wel degelijk over persoonsidentificerende gegevens betreffende prepaid bellers. Aan de hand van het nummer van de prepaid klant kan dan een relatie tussen verkeersgegevens en die persoonsidentificerende gegevens worden gelegd.”*¹⁹⁵

In haar zienswijze 1 geeft KPN aan dat ten aanzien van prepaid abonnees geldt dat verstrekking van NAW-gegevens niet verplicht is en dat zij niet over NAW-gegevens van al haar prepaid abonnees beschikt, zodat de verkeersgegevens niet als persoonsgegevens kunnen worden aangemerkt.¹⁹⁶

¹⁹² WP29 136. Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, p. 16-17.

¹⁹³ Idem, p. 22.

¹⁹⁴ Reactie KPN op verzoek om inlichtingen van 11 april 2012, p. 1.

¹⁹⁵ *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 80.

¹⁹⁶ Zienswijze 1 KPN, p. 13.

Ten aanzien van de prepaid abonnees van wie KPN geen NAW-gegevens en/of e-mailadressen heeft, beschikt KPN echter wel over ten minste het MSISDN (een direct contactgegevens), IMSI- en IMEI-nummer, in combinatie met onder andere IP-adres(sen)¹⁹⁷ en locatiegegevens met tijd.

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29-werkgroep over het begrip persoonsgegevens is hierover opgemerkt: *“(…) 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. (…) Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van “persoonsgegevens” weerspiegelt ook dit feit”, (onderstreping toegevoegd door het CBP).*¹⁹⁸

Wanneer gegevens gekoppeld worden aan een uniek nummer is doorgaans sprake van een geïndividualiseerd persoon. Het CBP verwijst in dat verband ook naar de overweging in het arrest van het Hof van Justitie van de EG van 6 november 2003 dat *“(…) 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, als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens in de zin van artikel 3, lid 1, van richtlijn 95/46 is aan te merken.”*¹⁹⁹

Zakelijke abonnees

Ook bedrijfsinformatie (bijvoorbeeld het telefoonnummer en bedrijfs-e-mailadres van een zakelijke abonnee die normaliter wordt gebruikt door een specifieke werknemer) is in een aantal gevallen als persoonsgegevens te beschouwen, bijvoorbeeld omdat de naam van de werknemer binnen dat bedrijf wordt vastgelegd.

¹⁹⁷ Zie HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), r.o. 26 over de status van IP-adressen, die persoonsgegevens vormen.

¹⁹⁸ WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 14-15.

¹⁹⁹ HvJ EG 6 november 2003, zaak C-101/01 (Lindqvist), r.o. 27.

Ook gegevens over eenmanszaken en bedrijven handelend onder een eigenaam worden als persoonsgegevens aangemerkt, wanneer die ook iets zeggen over het gedrag van de eigenaar.²⁰⁰

Gelet op het voorgaande zijn de in deze paragraaf genoemde gegevens van KPN abonnees met een (prepaid of postpaid) data abonnement op zichzelf (te weten: de unieke klant- en/of toestel identifier(s)), in onderlinge combinatie of in samenhang met uit andere bron bekende informatie, persoonsgegevens als bedoeld in artikel 1, onder a, van de Wbp.

De persoonsgegevens (informatie) over het communicatiegedrag van betrokkenen zijn gegevens van gevoelige aard. Het in kaart brengen van het surfgedrag van een natuurlijk persoon maakt inbreuk op de persoonlijke levenssfeer.²⁰¹

Verdere verwerking

KPN [VERTROUWELIJK] heeft de persoonsgegevens verder verwerkt door in april 2011 eenmalig een rapportage uit de [VERTROUWELIJK: apparatuur] met op persoonsniveau geaggregeerde²⁰² gegevens over het WhatsApp-gebruik door haar abonnees (inclusief de unieke IMSI-klantnummers van de betrokkenen)²⁰³ aan het KPN retailbedrijf te verstrekken voor marktonderzoek (analyse van de eigen dienstverlening).

Het KPN [VERTROUWELIJK] verstrekke sinds eind juli 2011 tot september 2012 periodiek rapportages uit de [VERTROUWELIJK: apparatuur] met op persoonsniveau geaggregeerde gegevens over het bezoek aan en gebruik door haar abonnees van een (groot) aantal apps en websites aan het KPN retailbedrijf, maar pas nadat uit de

²⁰⁰ Vgl. 'Klant in het web. Privacywaarborgen voor internettoegang', A&V-studie nr. 17, Registratiekamer juni 2000, p. 34 en 58. URL: http://www.cbppweb.nl/downloads_av/av17.pdf. Vgl. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 25. In deze opinie is verder opgemerkt over identificeerbaarheid: *"In die context wordt door de voor de verwerking verantwoordelijken vaak aangevoerd dat identificatie slechts zal plaatsvinden voor een gering percentage van het verzamelde materiaal en dat er dus vóór de identificatie in die paar gevallen plaatsvindt, geen sprake is van verwerking van persoonsgegevens. Het doel van videobewaking is echter de identificatie van de personen die op de videobeelden te zien zijn, in alle gevallen dat de voor de verwerking verantwoordelijke dat nodig acht. Het hele proces moet dan ook worden beschouwd als de verwerking van gegevens over identificeerbare personen, ook als sommige personen in de praktijk niet identificeerbaar zijn."* Idem, p. 17.

²⁰¹ Vgl. WP29 185, Opinion 13/2011 on Geolocation services on smart mobile devices van 16 mei 2011. URL: http://www.cbppweb.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. Zie Bevindingen Onderzoek door het College bescherming persoonsgegevens (CBP) naar de verwerking van persoonsgegevens door Advance Concepts B.V. van 15 december 2009, p. 27 en 28, URL: http://cbppweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf.

²⁰² Te weten: het aantal dagen waarop WhatsApp is gebruikt, de eerste en de laatste dag waarop WhatsApp is gebruikt en het totale aantal bytes dat met WhatsApp is uitgewisseld. Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3.

²⁰³ Over de periode februari-april 2011. Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

bestanden de IMSI-nummers van de betrokkenen waren verwijderd.²⁰⁴ Het CBP heeft vastgesteld dat deze geaggregeerde gegevens redelijkerwijs niet meer direct of indirect te herleiden zijn tot een natuurlijke persoon, niet door KPN of door enig ander persoon. Het zijn daarom in deze context geen persoonsgegevens.

Getroffen maatregelen: anonimiseringsoplossing

Het CBP heeft ten aanzien van de door KPN voorgestelde en gekozen anonimiseringsoplossing vastgesteld dat na het verstrijken van de 24-uurs periode de [VERTROUWELIJK] gegevens in beginsel niet meer herleidbaar zijn tot een identificeerbare natuurlijke persoon, niet door KPN en niet door een derde. [VERTROUWELIJK]. Er resteren geen unieke nummers of andere gegevens met persoonsidentificerende kenmerken van (de gebruiker van) het mobiele apparaat, behalve in het theoretische geval dat de bijkomende gegevens (bijvoorbeeld het IP-adres van de applicatieserver, gegevens over gebruik van apps [VERTROUWELIJK] door hun uniciteit direct of indirect herleidbaar zijn tot een individuele gebruiker. Het zijn daarom dan in deze context in beginsel geen persoonsgegevens meer. Tot dat moment zijn het persoonsgegevens die ook verkeersgegevens zijn, voor de verwerking waarvan een grondslag is vereist.

3.4 Verkeersgegevens versus communicatie

De gegevens over en uit het dataverkeer zijn tegelijkertijd zowel persoonsgegevens als gegevens betreffende elektronische communicatie.

Uitwerking van het wettelijk kader

In de Tw wordt onderscheid gemaakt tussen de begrippen ‘verkeersgegevens’ en ‘communicatie’.

Volgens artikel 11.1, aanhef en onder b, van de Tw wordt onder ‘verkeersgegevens’ verstaan: *gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.*

‘Communicatie’ is gedefinieerd in artikel 11.1, aanhef en onder e, van de Tw en omvat *informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische communicatiedienst.*

Artikel 11.1, aanhef en onder b, van de Tw, de definitie van het begrip ‘verkeersgegevens’, vormt een rechtstreekse omzetting van artikel 2, aanhef en onder b, van de e-Privacyrichtlijn. Artikel 11.1, aanhef en onder e, van de Tw, de definitie van het begrip ‘communicatie’, vormt een rechtstreekse omzetting van artikel 2, aanhef en onder d, van de e-Privacyrichtlijn.

De Europese wetgever heeft in (de toelichting op) overweging 15 van de e-Privacyrichtlijn onderkend dat *“het onderscheid tussen de inhoud van het communicatieverkeer en de desbetreffende verkeersgegevens niet meer zo duidelijk is als vroeger*

²⁰⁴ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3.

bij de traditionele spraaktelefonienetwerken. Dit is relevant voor de tenuitvoerlegging van de richtlijn."²⁰⁵

Overweging 15 van de e-Privacyrichtlijn luidt:

*"Een communicatie kan naamgevings-, nummerings- of adresseringsgegevens omvatten die door de verzender van een communicatie of door de gebruiker van een verbinding worden verstrekt om de communicatie tot stand te brengen. Wanneer deze gegevens door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren zij ook tot de verkeersgegevens. Verkeersgegevens kunnen o.a. gegevens zijn met betrekking tot de routing, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop communicatie begint of eindigt, het begin, het einde of de duur van de verbinding (...)"*²⁰⁶

Artikel 11.1, aanhef en onder c, van de Tw bepaalt dat de verwerking van verkeersgegevens een verwerking is als bedoeld in artikel 1, onder b, van de Wbp (met dien verstande dat de desbetreffende handelingen met betrekking tot verkeersgegevens van abonnees die geen natuurlijke personen zijn niet zonder meer persoonsgegevens zijn).

Of sprake is van persoonsgegevens die tevens verkeersgegevens zijn, is afhankelijk van het doel van de verwerking, te weten: voor het overbrengen van communicatie of voor andere doelen.²⁰⁷

In de wetsgeschiedenis bij de Tw is opgemerkt over persoonsgegevens die ook verkeersgegevens zijn: *"Het gaat niet om de inhoud van gesprekken maar om gegevens die inzicht kunnen geven in de contacten en het belgedrag van personen. (...) Dit neemt echter niet weg dat het hier gaat om persoonsgegevens en dat degene op wie de gegevens betrekking hebben het recht heeft op een zorgvuldige omgang met zijn gegevens, alsmede het recht op bescherming van zijn persoonlijke levenssfeer."*²⁰⁸

²⁰⁵ Mededeling van de Commissie aan het Europees Parlement over het gemeenschappelijk standpunt van de Raad met het oog op de vaststelling van een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie van 30 januari 2002 (SEC(2002)0124 def.).

²⁰⁶ Zie voor categorieën van verkeersgegevens in de sfeer van spraaktelefonie en internet: *Kamerstukken II 2003/04*, 28 851, nr. 3, p. 151; *Kamerstukken II 1998/99*, 25 892, nr. 6, p. 29; Bijlage bij artikel 13.2a van de Tw; *Kamerstukken 1997/98*, 25 533, nr. 5, p. 122; *Kamerstukken II 2000/01*, 27 460, nr. 2, p. 61; *Kamerstukken II 2002/03*, 28 962, nr. 3, p. 16.

"Abonneegegevens, zoals naam, adres, woonplaats, gegevens betreffende de wijze van betaling e.d. zijn wel nodig voor de facturering, maar vallen niet onder het begrip verkeersgegevens." Idem. Locatiegegevens kunnen verkeersgegevens zijn als deze gegevens ook vallen onder de definitie van verkeersgegevens van artikel 11.1, aanhef en onder b, van de Tw. *Kamerstukken II 2003/04*, 28 851, nr. 3, p. 47 en 151.

²⁰⁷ W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?', *Computerrecht* 2003, p. 28.

²⁰⁸ *Kamerstukken II 2007/08*, 31 145, nr. 9, p. 16-17.

Het begrip ‘communicatie’ ziet (daarentegen) op datgene wat wordt uitgewisseld dan wel overgebracht en niet op de gegevens die worden verwerkt om die uitwisseling of overbrenging mogelijk te maken, de zogeheten verkeersgegevens.

Zowel de inhoud van, als informatie over elektronische communicatie²⁰⁹ zijn gegevens die ook bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (Handvest).²¹⁰ Het Europees Hof voor de Rechten van de Mens (EHRM) oordeelde in zijn arrest van 3 april 2007 over de bescherming van e-mailcorrespondentie en internetgebruik:

*“Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8”, (onderstreping toegevoegd door het CBP).*²¹¹

Verkeersgegevens waaruit informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie volgt, zijn daarbij gegevens van gevoelige aard. In (de antwoorden op de vragen over) het kabinetsstandpunt over het rapport van de Commissie Grondrechten in het digitale tijdperk is hierover opgemerkt: *“Verkeersgegevens kunnen veel over personen zeggen. Dit geldt echter voor meer soorten van gevoelige gegevens.”*²¹²

Beoordeling

De begripsafbakening tussen ‘communicatie’ en ‘verkeersgegevens’ wordt bemoeilijkt door de steeds sterkere vervlechting van de gevoerde communicatie en de daarmee samenhangende gegevens in de technische protocollen. Bij spraaktelefonie kan het onderscheid tussen deze begrippen nog worden gemaakt langs de lijn van de

²⁰⁹ *“By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone”, (onderstreping toegevoegd door het CBP). EHRM 2 augustus 1984, NJ 1988, 534 (Malone).*

²¹⁰ De in artikel 7 van het Handvest gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) zijn gewaarborgd. Dit recht heeft dezelfde inhoud en reikwijdte als het recht in de daarmee corresponderende bepaling van het EVRM. Artikel 8 van het Handvest is een afzonderlijke bepaling over de bescherming van persoonsgegevens. Toelichtingen bij het Handvest van de grondrechten. URL: <http://eur-lex.europa.eu/nl/treaties/dat/32007X1214/htm/C2007303NL.01001701.htm> (URL laatst bezocht op 29 mei 2013). Het CBP heeft (daarom) in zijn wetgevingsadvies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet van 11 februari 2013 geadviseerd nadere aandacht te schenken aan de reikwijdte van het voorgestelde artikel 13 van de Grondwet (de uitzondering voor verkeersgegevens). URL: http://www.cbpreweb.nl/Pages/adv_z2012-00746.aspx (URL laatst bezocht op 29 mei 2013).

²¹¹ EHRM 3 april 2007, NJ 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44.

²¹² *Kamerstukken II 2000/01, 27 460, nr. 2, p. 61. Zie ook idem, nr. 1, p. 27: “(...) het feit dat verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens (...).”*

technische scheiding tussen spraak- (dat wat wordt gezegd) en signaleringskanaal (dat wat nodig is om de verbinding tot stand te brengen). Bij communicatietoepassingen zoals mobiele telefonie en internet is dat niet langer zonder meer het geval (http bevat zowel inhoudskenmerken als verkeersgegevens).

De opsomming in overweging 15 van de e-Privacyrichtlijn en de wetsgeschiedenis²¹³ geeft een indicatie welke categorieën van gegevens over het dataverkeer als verkeersgegevens moeten worden aangemerkt. Beide noemen onder andere de routing, de duur, het tijdstip, het volume van de communicatie, het gebruikte protocol en de locatiegegevens als gegevens die door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen.

Ook ten aanzien van de hostname (URL op hoofddomein) en de referer (laatst bezochte URL), geldt dat deze door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen. Dat het strikt genomen mogelijk is om onderscheid te maken tussen de inhoudelijke vraag (Get request URL) en de nummerreeks van de webserver (IP-adres), maakt dat niet anders. Om een webpagina op te roepen vindt de volgende gegevensuitwisseling plaats. Een gebruiker toetst een URL in, die door de Domain Name Server (DNS) wordt vertaald naar het bijbehorende IP-adres. Vervolgens wordt de webserver benaderd die de webpagina herbergt.

De gegevens over het dataverkeer zijn (derhalve) zulke verkeersgegevens (die ook persoonsgegevens zijn), voor zover er daadwerkelijke communicatie plaatsvindt.²¹⁴

De verkeersgegevens over het communicatiegedrag van betrokkenen (URL's) zijn gegevens van gevoelige aard.²¹⁵ De URL heeft in de meeste gevallen ook een inhoudelijke waarde, in die zin dat daaruit informatie is af te lezen over de communicatie-inhoud. URL's vallen (daarom) ook niet onder de bewaarplicht verkeersgegevens. Websurfgedrag (informatie over bezochte sites) is daarvan uitgezonderd. In de wetsgeschiedenis bij de Wet bewaarplicht telecommunicatiegegevens is daarover opgemerkt: *“Op grond van de richtlijn moeten alleen de gegevens betreffende internettoegang bewaard worden en niet de gegevens over het*

²¹³ Zie *Kamerstukken II 1998/99*, 25 892, nr. 6, p. 29; *Kamerstukken II 2002/03*, 28 851, nr. 3, p. 151; *Kamerstukken II 2000/01*, 27 460, nr. 2, p. 61, *Kamerstukken II 2002/03*, 28 962, nr. 3, p. 16. Zie ook Bijlage bij artikel 13.2a van de Tw.

²¹⁴ Voor zover ten aanzien van een toestel in stand-by stand (oftewel: *idle mode*) onder andere locatiegegevens worden verzonden over het signaleringskanaal om ervoor te zorgen dat het op elk moment inkomende berichten kan ontvangen, geldt dat geen sprake is van verkeersgegevens (alleen maar van persoonsgegevens) omdat er geen communicatie wordt/is gevoerd. Vgl. M.G.M. Hoegendijk, *Zakboek Strafvordering voor de Hulpofficier 2011/9.14*, p. 5; T&C Strafvordering, commentaar op artikel 126n Sv. De Hoge Raad heeft overwogen in zijn arrest van 7 september 2004: *“(…) [onder inlichtingen ter zake van alle verkeer, oftewel verkeersgegevens, vallen, toevoeging door het CBP] gegevens betreffende de locatie van een gebruiker van een telecommunicatiemiddel, althans indien en voor zover deze het middel ook daadwerkelijk gebruikt en aan het telecommunicatieverkeer deelneemt.”* HR 7 september 2004, NJ 2004, 610. Gegevens die in idle mode over het signaleringskanaal worden verzonden vallen buiten de scope van dit onderzoek.

²¹⁵ *Kamerstukken II 2000/01*, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.

websurfgedrag."²¹⁶ En: "Het gaat niet om het opslaan van websites die zijn bezocht."²¹⁷ De Wet bewaarplicht telecommunicatiegegevens vormt een implementatie van de richtlijn betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten 2006/24/EG (Dataretentierichtlijn). Artikel 1, tweede lid, van de Dataretentierichtlijn luidt: "Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Zij is niet van toepassing op de inhoud van elektronische communicatie, de informatie die wordt geraadpleegd met behulp van een elektronisch communicatienetwerk daaronder begrepen." Artikel 5, tweede lid, van de Dataretentierichtlijn bepaalt: "Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mogen krachtens deze richtlijn niet worden bewaard."

Ten aanzien van zogeheten *signature based protocollen*, geldt dat signature based data analyse ten behoeve van protocol of appherkenning (zoals voip, p2p, of specifieke apps als Skype) plaatsvindt door onderscheidende kenmerken te gebruiken die onderdeel zijn van de applicatielaag van het internetverkeer.

Deze kenmerken worden herkend in de initiatiefase van het protocol, bij het opzetten van de verbinding.

In de initiatiefase van een applicatieprotocol worden over het algemeen gegevens vervoerd die nodig zijn om de communicatie tot stand te brengen. Dat daartoe via het TCP en IP protocol uit de onderliggende internet- en transportlagen ook al packets worden vervoerd die gegevens uit de applicatielaag bevatten, betekent niet dat die pakketten dus communicatiegegevens bevatten.

Omdat het niet mogelijk is om vooraf te bepalen wanneer de initiatiefase begint, zullen in beginsel alle headers en de eerste paar packets vergeleken worden met de signature. Op het moment dat er een match is tussen een signature en een packet, is het niet meer nodig om verder te vergelijken. Gelet op het voorgaande worden deze gegevens beoordeeld als verkeersgegevens, tevens persoonsgegevens.

(Louter) gegevens uit het dataverkeer zijn communicatie tevens persoonsgegevens. Ten aanzien van spam-, virus- en malwareherkenningsgegevens uit (gedownloade) bestanden en verzonden en ontvangen e-mails geldt, voor zover KPN deze verwerkt om spam en malware/virussen tegen te houden en te verwijderen, dat geen sprake is van verkeersgegevens, maar van zulke communicatie (de bestanden en berichten die worden overgebracht).²¹⁸

Samengevat, kunnen de persoonsgegevens worden ingedeeld in twee categorieën:

²¹⁶ *Kamerstukken I* 2008/09, 31 145, C, p. 17. Zie in dezelfde zin idem, p. 12.

²¹⁷ *Handelingen II* 2007/08, 83, p. 5836.

²¹⁸ Het CBP heeft bovenstaande toepassing van de begrippen 'communicatie' en 'verkeersgegevens' voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom – College bescherming persoonsgegevens van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van deze begrippen in dit rapport.

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het telefoonnummer), zendmastgegevens (Cell ID), de starttijd en eindtijd van de data sessie, verbruikte datavolume, URL's etc.
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

3.5 Gegevensverwerking

Uitwerking van het wettelijk kader

Het begrip 'verwerking van persoonsgegevens' als bedoeld in artikel 1, onder b, van de Wbp omvat het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen tot aan het moment van vernietiging.²¹⁹ Ook het genereren van persoonsgegevens is een verwerking.²²⁰ Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze gegevens.²²¹ Ook volledig geautomatiseerde vormen van gegevensverwerking vormen een verwerking, zo lang (enige) invloed daarop uit kan worden geoefend. De verwerking van verkeersgegevens is een verwerking van persoonsgegevens (artikel 11.1, aanhef en onder c, van de Tw).²²² Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen (*mere conduit*), verwerkt daarmee geen persoonsgegevens.²²³

Beoordeling

Het CBP heeft in paragrafen 2.4 tot en met 2.7 (p. 21 e.v. van dit rapport) vastgesteld dat KPN meer doet dan alleen maar gegevens doorvoeren/doorgeven (afhankelijk van het verwerkingsdoel: inspecteren/genereren, gebruiken (waaronder in dit geval ook begrepen analyseren) en soms ook vastleggen en bewaren). KPN verwerkt (aldus) persoonsgegevens die (in de meeste gevallen) ook verkeersgegevens zijn. Er is geen sprake van een *mere conduit*-uitzondering.

Ofwel KPN verkrijgt (verzamelt) de persoonsgegevens via het gebruik van data-analyse technieken. Zo inspecteert/inspecteerde KPN (i) tot 21 september 2012 voor

²¹⁹ Zie *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 51-52.

²²⁰ Idem, p. 51

²²¹ 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.

²²² Met dien verstande dat de desbetreffende handelingen met betrekking tot verkeersgegevens van abonnees die geen natuurlijke personen zijn niet zonder meer persoonsgegevens zijn.

²²³ Idem: "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). Idem, p. 51-52.

netwerkplanning en -beheer gegevens in het eerste datapakket dat van het toestel van de abonnee naar de applicatieserver ging, (ii) tot 3 oktober 2012 voor het faciliteren van opwaardeermogelijkheden URL's om de (gratis) opwaardeersites te herkennen, (iii) voor spam- en virusbestrijding (gedownload) bestanden en verzonden en ontvangen e-mails om spam/ virussen/malware tegen te houden en te verwijderen en (iv) voor de behandeling van klantklachten het dataverkeer op bijvoorbeeld (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan (ordering van al aanwezige gegevens).²²⁴ Ofwel KPN analyseert/analyseerde via het gebruik van data-analyse technieken persoonsgegevens die worden aangemaakt in haar mobiele netwerk (bijvoorbeeld dataverbruik gegevens om te kunnen factureren).

Gelet op het voorgaande verwerkt (e) KPN persoonsgegevens als bedoeld in artikel 1, onder b, van de Wbp .

3.6 Grondslag

Uitwerking van het wettelijk kader

Artikel 5 van de e-Privacyrichtlijn regelt het vertrouwelijk karakter van de communicatie.

Artikel 5 van de e-Privacyrichtlijn bepaalt (kort gezegd), voor zover voor dit onderzoek van belang: de lidstaten verbieden het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit laat onverlet de technische opslag die nodig is voor het overbrengen van informatie, onverminderd het vertrouwelijkheidsbeginsel, en de bij de wet toegestane registratie van communicatie en de daarmee verband houdende verkeersgegevens, wanneer die wordt uitgevoerd in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van enigerlei andere zakelijke communicatie.

Artikel 11.2a van de Tw (nieuw) dient ter implementatie van artikel 5 van de e-Privacyrichtlijn.²²⁵

Artikel 11.2a, tweede lid, onder a tot en met d, van de Tw bepaalt, voor zover voor dit onderzoek van belang: *de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst onthouden zich van het aftappen, afluisteren of anderszins onderscheppen of controleren van de communicatie via een openbaar elektronisch communicatienetwerk of openbare elektronische communicatiedienst en de daarmee verband houdende gegevens tenzij en voor zover:*

- a. de betrokken abonnee voor deze handelingen zijn uitdrukkelijke toestemming heeft gegeven;*
- b. deze handelingen noodzakelijk zijn om de integriteit en de veiligheid van de netwerken en diensten van de betrokken aanbieder te waarborgen;*
- c. deze handelingen noodzakelijk zijn voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder, of*

²²⁴ Kamerstukken II 1997/98, 25 892, nr. 3, p. 68.

²²⁵ Kamerstukken I 2011/12, 32 549, E, p. 2.

d. deze handelingen noodzakelijk zijn ter uitvoering van een wettelijk voorschrift of rechterlijk bevel.

Als hoofdregel geldt op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het af luisteren, aftappen, op slaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers verboden is, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit artikel geeft aldus een verwerkingsverbod, met uitzonderingen. Op deze eerder genoemde hoofdregel is in lid 2 van artikel 11.2a van de Tw bijvoorbeeld een uitzondering geformuleerd voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder.

In de wetsgeschiedenis bij artikel 11.2a is opgemerkt over *Deep Packet Inspection* (hierna: DPI): “Artikel 11.2a Tw ziet op de vertrouwelijkheid van de communicatie die via internet of andere elektronische communicatiediensten of -netwerken plaats vindt. Dit artikel waarborgt aldus dat de vertrouwelijkheid van de communicatie van bedrijven en consumenten, bijvoorbeeld via internet, wordt gewaarborgd. Overigens verbiedt artikel 11.2a Tw in den brede het aftappen of af luisteren, en dergelijke van communicatie door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, dus ook wanneer dit plaats heeft met een andere methode dan de methode van Deep Packet Inspection. Bezien vanuit de positie van de aanbieders van elektronische communicatienetwerken en diensten stellen beide artikelen grenzen aan het beheer van de door hen aangeboden netwerken en diensten. Belangrijk op te merken is dat zowel artikel 7.4a als artikel 11.2a Tw (zie met name tweede lid, onder b en c) er niet aan in de weg staan dat een aanbieder zijn netwerk en diensten op een «normale» manier beheert. Zo mag, ook in het kader van artikel 11.2a Tw (zie tweede lid, onder c), een aanbieder van een netwerk om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is de diverse verkeersstromen die over dat netwerk worden afgewikkeld in kaart brengen. Hij mag in dat kader, bijvoorbeeld, gegevens verzamelen over het volume van het verkeer van bepaalde diensten of applicaties, het aantal keren dat verbinding wordt gemaakt et cetera. Wel is belangrijk dat het verzamelen van dergelijke gegevens niet verder gaat dan nodig is voor het goed laten functioneren van het netwerk en de daarover afgewikkelde diensten. Ook laten beide artikelen toe dat maatregelen worden genomen ter voorkoming van congestie. Zo staat artikel 11.2a Tw (zie het tweede lid, onder c) noch artikel 7.4a Tw er aan in de weg dat een aanbieder kijkt of hij te maken heeft met een VOIP dienst of een e-mail dienst om deze vervolgens om voor de hand liggende redenen (pakketverlies maakt een e-mail onleesbaar maar enige vertraging is geen probleem, bij VOIP verkeer is dit juist andersom) bij congestie verschillend te behandelen”, (onderstreping toegevoegd door het CBP).²²⁶

De leden van de CDA-fractie hebben opgemerkt in de wetsgeschiedenis bij dit artikel 11.2a van de Tw: “De leden van de CDA-fractie stemmen in met de conclusie van de regering dat het bepaalde in het bij amendement ingevoegde artikel 11.2a geen nieuwe beperkingen aan aanbieders zou moeten opleggen voor een adequaat netwerkbeheer. Het gaat in artikel 5 van de e-Privacy-richtlijn - waarvan de bepaling een implementatie beoogt te zijn - om de bescherming van «het vertrouwelijke karakter van de communicatie». Vooral bij mobiele netwerken is er thans een zo snelle ontwikkeling van verschillende applicaties, randapparatuur en dergelijke, dat netwerkaanbieders voor een goed beheer moeten kunnen controleren welke applicaties en

²²⁶ Kamerstukken I 2011/12, 32 549, E, p. 13.

apparatuur worden gebruikt en hoe die zich in de netwerken gedragen, zonder dat ze daarmee kennis nemen van de inhoud van de via die applicaties verzonden communicatie. De bepaling moet - zo merken de leden van de CDA-fractie op - niet zover worden opgerekt dat ook die - noodzakelijke - «controle» van het soort verkeer (zonder kennisname van de inhoud) onder de verbodsbepaling valt.”²²⁷

Dit alles betekent dat artikel 11.2a van de Tw er niet aan in de weg staat dat een aanbieder van een netwerk gegevens *verzamelt* over het volume van het verkeer van bepaalde diensten of applicaties, het aantal keren dat verbinding wordt gemaakt etc. om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is, mits het verzamelen van dergelijke gegevens niet verder gaat dan nodig is voor het goed laten functioneren van het netwerk en de daarover afgewikkelde diensten (proportionaliteitstoets).

In de toelichting op het bij amendement ingevoegde artikel 11.2a is opgemerkt over proportionaliteit: *“Lid 2 bevat een algemeen verbod op het meeluisteren naar verkeer dat via aanbieders wordt getransporteerd, behalve in het geval dat specifiek omschreven uitzonderingen van toepassing zijn. Niet alleen het opslaan, maar ook het zonder opslag analyseren van communicatie is onder dit lid verboden. De uitzonderingen onder a tot en met d moeten beperkt worden uitgelegd, zoals ook blijkt uit de woorden «indien en voor zover». Hiermee willen de indieners onderstrepen dat een uitzondering nooit verder mag gaan dan noodzakelijk, en dus moet voldoen aan strikte eisen van proportionaliteit. Ook het gebruik van de term «noodzakelijk» in de uitzonderingen is bedoeld om deze toets te onderstrepen. De uitzondering onder a is erop gericht om de abonnee de vrijheid te laten ervoor te kiezen dat zijn communicatie wordt geanalyseerd.”²²⁸*

Het artikel geeft bovendien op zichzelf geen grondslag voor de *verwerking* van de communicatie én de daarmee verband houdende verkeersgegevens die ook persoonsgegevens zijn (maar uitzonderingen op het verwerkingsverbod). Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil verzamelen voor de in artikel 11.2a van de Tw genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Persoonsgegevens die ook verkeersgegevens zijn

Artikel 11.5 van de Tw vormt een implementatie van artikel 6 van de e-Privacyrichtlijn en geeft regels voor de verwerking van verkeersgegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten.

Artikel 11.5, eerste tot en met derde en vijfde lid, van de Tw luidt, voor zover voor dit onderzoek van belang:

1. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst verwijderen dan wel anonimiseren de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie, onverminderd het tweede, derde en vijfde lid.

²²⁷ Kamerstukken I 2011/12, 32 549, F, p. 5.

²²⁸ Kamerstukken II 2010–2011, 32 549, nr. 16, p. 2-3.

2. De aanbieder mag verkeersgegevens verwerken die noodzakelijk zijn voor facturering, waaronder het opstellen van een factuur voor een abonnee of voor degene die zich tegenover de aanbieder rechtens verbonden heeft die factuur te voldoen, dan wel ten behoeve van een betaling van verleende toegang. De verkeersgegevens mogen worden verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen.

3. De aanbieder van elektronische communicatiediensten mag voorts de in het eerste lid bedoelde verkeersgegevens verwerken, voor zover en voor zolang dat noodzakelijk is voor:

a. marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, of

b. de levering van diensten met toegevoegde waarde, mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor voorafgaand aan de verwerking zijn toestemming heeft gegeven. (...) ²²⁹

5. De verwerking van verkeersgegevens in overeenstemming met het eerste tot en met vierde lid mag alleen geschieden door personen die werkzaam zijn onder het gezag van de aanbieder voor facturering, verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude alsmede marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.
(...)

‘Dienst met toegevoegde waarde’ is gedefinieerd in artikel 11.1, aanhef en onder h, van de Tw: dienst die de verwerking vereist van verkeersgegevens of locatiegegevens, niet zijnde verkeersgegevens, en die verder gaat dan hetgeen noodzakelijk is voor de overbrenging van een communicatie of de facturering daarvan.

Overbrenging van communicatie

De hoofdregel uit artikel 11.5 van de Tw is dat alle door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees en gebruikers worden verwijderd dan wel geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. ²³⁰ Voor dataverkeer is dit bijvoorbeeld afhankelijk van het type dienst. ²³¹

Onder het begrip ‘anonimiseren’ wordt verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende

²²⁹ Per 5 juni 2012 is in dit derde lid “mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor zijn toestemming heeft gegeven” vervangen door: mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor voorafgaand aan de verwerking zijn toestemming heeft gegeven. *Stb.* 2012, 235 en 236.

²³⁰ *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 154.

²³¹ *Idem*, p. 154-155: “Waar het gaat om websurfen ligt de zaak in zoverre eenvoudiger dat het moment van verwijderen of anonimiseren voor de desbetreffende aanbieder aanbreekt op het moment dat deze de verbinding met het internet (in de betekenis van het surfen op het World Wide Web) verbreekt; dit laatste hoeft niet altijd samen te vallen met beëindiging van de verbinding met de dienstenaanbieder, waarbij men bijvoorbeeld aansluitend diens e-mail account (account voor elektronische post) kan gaan bekijken.” Zie ook overweging 27 van de e-Privacyrichtlijn.

kenmerken.²³² De gegevens moeten zodanig worden bewerkt dat ze redelijkerwijs niet meer zijn te herleiden naar individuele natuurlijke personen. Het verwijderen van de direct persoonsidentificerende kenmerken biedt op zichzelf niet altijd voldoende garantie dat geen sprake meer is van persoonsgegevens.²³³ Het kan nodig zijn dat er andere, aanvullende maatregelen worden getroffen om herleidbaarheid van de gegevens te voorkomen.

Overweging 30 van de e-Privacyrichtlijn luidt in dit verband:

“Systemen voor elektronische-communicatienetwerken en -diensten moeten op dusdanige wijze worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. Activiteiten die betrekking hebben op het aanbieden van elektronische-communicatiediensten en verder gaan dan de transmissie van communicatie en de facturering ervan moeten gebaseerd worden op geaggregeerde verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht. Indien deze activiteiten niet op geaggregeerde gegevens kunnen worden gebaseerd, moeten ze als diensten met toegevoegde waarde worden aangemerkt, waarvoor toestemming van de abonnee vereist is”, (onderstreping toegevoegd door het CBP).

Facturering, verkeersbeheer en behandeling van verzoeken om inlichtingen van abonnees

De (Europese) wetgever heeft beoogd het begrip ‘facturering’ een ruime betekenis te geven. Onder de verwerking ten behoeve van de facturering wordt niet alleen het opstellen van een factuur begrepen, maar ook bijvoorbeeld het registreren van het beltegoed van prepaid abonnees (en betaling van verleende toegang).²³⁴ In de wetsgeschiedenis bij de Tw wordt daarover opgemerkt: *“Daarmee komt ook buiten kijf te staan dat de verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed; dit laatste dient onder facturering te worden begrepen.”*²³⁵

Overweging 13 van de e-Privacyrichtlijn luidt in dit verband:

“De contractuele relatie tussen een abonnee en een dienstenaanbieder kan een periodieke of een eenmalige betaling voor de verleende of de te verlenen dienst inhouden. Ook vooruitbetaalde kaarten worden beschouwd als een contract.”

Onder ‘overbrenging van communicatie’ en ‘facturering’ moet ook verkeersbeheer, behandeling van verzoeken om inlichtingen van abonnees en opsporing van fraude worden begrepen (zie onder andere artikel 11.5, vijfde lid, van de Tw jo. overweging 29 van de e-Privacyrichtlijn).²³⁶ Het gaat hier niet om zelfstandige verwerkingsdoelen, maar om verwerkingsdoelen die van het factureringsdoel en het overbrengen van de

²³² Idem, nr. 7, p. 80.

²³³ Kamerstukken II 1997/98, 25 892, nr. 3, p. 48.

²³⁴ Kamerstukken II 2002/03, 28 851, nr. 3, p. 155.

²³⁵ Idem, nr. 13, p. 20.

²³⁶ Idem, nr. 3, p. 156.

communicatie zijn afgeleid.²³⁷ De verkeersgegevens mogen (ook) voor die (afgeleide) doelen worden verwerkt, voor zover noodzakelijk.

De verwerking van niet-geanonimiseerde verkeersgegevens is toelaatbaar indien (lees: zolang) deze noodzakelijk is voor de hierboven genoemde verwerkingsdoelen.

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” (...).”*²³⁸

Het Hof van Justitie van de EG vult het begrip noodzakelijkheid, ‘een autonoom begrip van gemeenschapsrecht’, op een strikte wijze in.²³⁹ Uit een arrest van het Hof van Justitie van de EG van 16 december 2008 volgt dat indien het (enige) doel de vergaring van statistische gegevens is, het niet noodzakelijk is de (persoons)gegevens op naam te bewaren en te verwerken.²⁴⁰

Ten aanzien van de verwerking ten behoeve van de facturering geldt dat het noodzakelijkheids criterium nader wordt ingevuld doordat is bepaald dat de verwerking is toegestaan tot het einde van de termijn waarbinnen de factuur in rechte kan worden betwist dan wel de betaling in rechte kan worden afgedwongen.²⁴¹ Dit betekent niet dat in alle gevallen - ongeacht of er sprake is van wel of niet betaling of wel of niet betwisting van de factuur - de verkeersgegevens tot het einde van die termijn mogen worden bewaard. In de gevallen dat de factuur is betaald en er voor het overige daaromtrent geen geschillen ontstaan, is het niet nodig de desbetreffende verkeersgegevens langer voor dat doel te bewaren.²⁴²

Marktonderzoek/verkoopactiviteiten en toegevoegde waardedienst

Verkeersgegevens mogen ook worden verwerkt ten behoeve van marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde, mits de betrokken abonnee of gebruiker daarvoor zijn toestemming heeft gegeven. Toestemming van een gebruiker

²³⁷ Idem.

²³⁸ EHRM 25 maart 1983, nr. 97 (Silver & Others v. United Kingdom).

²³⁹ Vgl. ook HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 52.

²⁴⁰ HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 64-65 en 68: *“Evenzo gaat verordening nr. 862/2007, die de verstrekking regelt van van statistische gegevens over de migratiebewegingen op het grondgebied van de lidstaten, ervan uit dat de lidstaten de informatie verzamelen op basis waarvan die statistieken kunnen worden opgesteld. De uitoefening van die bevoegdheid maakt echter niet het verzamelen en bewaren van gegevens op naam zoals plaatsvindt in het kader van een register als het AZR, noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46. Zoals de advocaat-generaal in punt 23 van zijn conclusie heeft aangegeven, is voor een dergelijk doel alleen de verwerking van anonieme gegevens noodzakelijk. (...) In geen geval kunnen als noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46 worden beschouwd de bewaring en de verwerking van persoonsgegevens op naam in het kader van een register als het AZR, voor statistiekdoeleinden.”* Vgl. AG HvJ 3 april 2008, zaak C-524/06 (Huber), r.o. 23: *“Statistieken zijn per definitie anoniem en niet persoonsgebonden.”*

²⁴¹ Idem, p. 155. In veel gevallen zal dat neerkomen op een termijn van ten hoogste vijf jaar (artikel 3:307 e.v. van het Burgerlijk Wetboek).

²⁴² Idem.

of abonnee 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).²⁴³

Uit de wetsgeschiedenis bij de Tw blijkt dat artikel 11.5 van de Tw is bedoeld als uitputtende regeling: *"In artikel 11.5 van de wet worden aan de verwerking van verkeersgegevens specifieke voorwaarden gesteld en voor zover het daarbij gaat om de verwerking van persoonsgegevens dienen die als een specialis ten opzichte van de algemene normen uit de Wbp ter zake te worden aangemerkt."*²⁴⁴

Voor het verwerken van persoonsgegevens is (desondanks) 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;*

(...)

- 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.*

Artikel 11.5 van de Tw geeft, voor zover voor dit onderzoek van belang, op dit punt een nadere begrenzing/inperking van de toegestane verwerkingen van verkeersgegevens, tevens persoonsgegevens in de sector elektronische communicatie.²⁴⁵

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, zonder economische dwang.²⁴⁶ 'Specifiek' betekent dat de

²⁴³ Het CBP heeft bovenstaande uitleg van artikel 11.5 van de Tw voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom-CBP van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van dit artikel in dit rapport.

²⁴⁴ *Kamerstukken II 2002/03, 28 851, nr. 7, p. 54. Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 6.*

²⁴⁵ Zie artikel 1, tweede lid, en overweging 12 van de e-Privacyrichtlijn. Zie ook *Kamerstukken II 2002/03, 28 851, nr. 7, p. 53; Kamerstukken I 1997/98, 25 533, nr. 5, p. 115 en Kamerstukken I 1997/98, 25 533, nr. 309d, p. 8; Kamerstukken II 2002/03, 28 851, nr. 3, p. 59.*

²⁴⁶ *Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.*

wilsuïting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).²⁴⁷ ‘Geïnformeerd’ betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.²⁴⁸

Van *ondubbelzinnige* toestemming is slechts sprake indien bij de verantwoordelijke elke twijfel is uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.²⁴⁹ ‘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).²⁵⁰ 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.”²⁵¹

In de opinie van de Artikel 29-werkgroep is over ‘ondubbelzinnige toestemming’ verder aangegeven:

“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.”²⁵²

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.²⁵³ Daarbij geldt als voorwaarde dat het moet gaan om

²⁴⁷ Idem. In de opinie 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.” WP29 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/index_en.htm.

²⁴⁸ Idem.

²⁴⁹ Idem, p. 80.

²⁵⁰ Idem, p. 66 en 67. Zie ook WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 28 en 41.

²⁵¹ *Handelingen I* 1999/2000, 34, p. 1632. Vgl. ook HvJ EU van 19 juli 2012, zaak C112/11 (ebookers.com), r.o. 16 en HvJ EU van 9 november 2010, zaaknummers C-92/09 en C-93/09.

²⁵² WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 41.

²⁵³ *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80.

een overeenkomst waarbij de betrokkene partij is²⁵⁴ en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (dat wil zeggen: als de overeenkomst niet goed kan worden uitgevoerd zonder de persoonsgegevens).²⁵⁵

De uitgever van een krant mag bijvoorbeeld de persoonsgegevens van zijn abonnees verwerken omdat dat noodzakelijk is om de krant te kunnen bezorgen²⁵⁶ (zonder NAW-gegevens van de betreffende 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).²⁵⁷ De grondslag is strikt beperkt tot de gegevens die voor de uitvoering van de overeenkomst noodzakelijk zijn.

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*.²⁵⁸ 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 plicht

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.²⁵⁹ 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

²⁵⁴ 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.

²⁵⁵ Kamerstukken II 1997/98, 25 892, nr. 3, p. 81.

²⁵⁶ Handleiding voor verwerkers van persoonsgegevens. Wet bescherming persoonsgegevens, Ministerie van Justitie, Den Haag: 2002, p. 22. URL: <http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html>.

²⁵⁷ 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).

²⁵⁸ 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.”

²⁵⁹ 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.

verplichting redelijkerwijs niet goed mogelijk zijn; proportionaliteits- en subsidiariteitstoets).²⁶⁰ Anders gezegd: er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.²⁶¹ Daarbij moet onder andere worden gelet op de aard van de in het geding zijnde taak en de aard van de betrokken persoonsgegevens.²⁶² 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.²⁶³ 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.²⁶⁴

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 verrichten²⁶⁵) 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. 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 kan niet anderszins of met minder ingrijpende middelen worden bereikt (subsidiariteitstoets).²⁶⁶

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.²⁶⁷ 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.²⁶⁸

Uit de wetsgeschiedenis bij de Wbp kan wel worden afgeleid dat artikel 8 van de Wbp een uitputtende opsomming geeft van verwerkingsgronden: *“Artikel 7 betreft de verzameling van persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en*

²⁶⁰ Idem, p. 82-83. Een verwerking die uitsluitend dient ter uitvoering van een wettelijk recht valt hier buiten.

²⁶¹ Idem, p. 82.

²⁶² Idem, p. 83.

²⁶³ Idem.

²⁶⁴ Idem.

²⁶⁵ Idem, p. 86.

²⁶⁶ 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.

²⁶⁷ *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 87.

²⁶⁸ Idem.

gerechtvaardigde doeleinden. Hierop zijn geen uitzonderingen. Hetzelfde geldt voor de in artikel 8 genoemde gronden op basis waarvan persoonsgegevens mogen worden verwerkt. Artikel 8 omvat derhalve een uitputtende opsomming van verwerkingsgronden.”²⁶⁹

Als hoofdregel geldt op grond van artikel 11.5, eerste lid, van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer nodig/noodzakelijk zijn ten behoeve van (het doel van) de overbrenging van communicatie (inclusief de afgeleide doeleinden verkeersbeheer en behandeling van verzoeken om inlichtingen van klanten etc.) (proportionaliteitstoets). Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor facturering, of voor marktonderzoek/verkoopactiviteiten en toegevoegde waardediensten mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor toestemming heeft gegeven).

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp²⁷⁰ op het punt van de bevoegdheid tot (toelaatbaarheid van) het bewaren van persoonsgegevens die ook verkeersgegevens zijn (oftewel, een verplichting tot verwijdering dan wel anonimisering van gegevens, met uitzonderingen).²⁷¹ Dit artikel geeft echter op zichzelf geen grondslag voor de verwerking van de niet verwijderde of niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn (maar uitzonderingen op de verwijderings-/anonimiseringsplicht).²⁷² Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp.

Wel geeft de uitputtende regeling in artikel 11.5 van de Tw een nadere begrenzing/inperking van de toegestane verwerkingen van persoonsgegevens die ook

²⁶⁹ *Kamerstukken II 1998/99, 25 892, nr. 13, p. 5-6.*

²⁷⁰ Te weten: het vereiste dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

²⁷¹ T&C Telecommunicatierecht, commentaar op artikel 11.5 Telecommunicatiewet en T&C Telecommunicatierecht, commentaar op artikel 10 WBP. Vgl. ook M.J.T. Artz & M.M.M. van Eijk, *Klant in het web. Privacywaarborgen voor internettoegang* (Achtergrondstudies en verkenningen 17), Registratiekamer juni 2000, p. 27.

²⁷² Vgl. de verbods- en ontheffingssystematiek ten aanzien van de verwerking van bijzondere persoonsgegevens (artikel 16 e.v. van de Wbp). In de wetsgeschiedenis bij de Wbp is daarover het volgende opgemerkt “Artikel 16 is conform de richtlijn geformuleerd als een verbod. Dit impliceert dat als hoofdregel geldt dat verwerking van gevoelige gegevens niet is toegestaan. De daarop volgende bepalingen (artikel 17 tot en met 23) zijn in dezelfde sleutel geplaatst en geformuleerd als een ontheffing van het algemene verwerkingsverbod. Langs deze weg wordt ook tot uitdrukking gebracht dat artikel 17 e.v. niet zonder meer legitimeren tot gegevensverwerking: zij doorbreken slechts een verbod. Vervolgens zal aan de hand van de algemene beginselen van gegevensverwerking - zoals vastgelegd in artikel 6 tot en met 15 van het wetsvoorstel - moeten worden vastgesteld of de gegevensverwerking in het concrete geval rechtmatig is”, (onderstreping toegevoegd door het CBP). *Kamerstukken II 1997/98, 25 892, nr. 3, p. 101.*

verkeersgegevens zijn in de telecommunicatiesector, namelijk waar het gaat om de vraag of (lees: hoe lang) een grondslag is te vinden in de Wbp voor de verwerking van niet verwijderde of niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn. Het CBP toetst de beoordeling van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn derhalve aan artikel 11.5 van de Tw jo. artikel 8 van de Wbp. Dat betekent materieel (inhoudelijk) dat als de gegevensverwerking is toegestaan onder artikel 11.5 van de Tw ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de Tw ook geen grondslag is te vinden in de Wbp.

Persoonsgegevens die ook communicatie betreffen

Ten aanzien van de verwerking van communicatie, tevens persoonsgegevens geldt het volgende.

Artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) geeft een verplichting voor de aanbieder van een openbare elektronische communicatiedienst en -netwerk om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Dit artikel 11.3 van de Tw stelt eisen aan de beveiliging van persoonsgegevens en geeft aldus een telecomspecifieke uitwerking van artikel 13 van de Wbp.²⁷³ Het artikel geeft (dus) geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

Als hoofdregel geldt op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers verboden is, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit artikel geeft aldus een verwerkingsverbod, met uitzonderingen. Op deze eerder genoemde hoofdregel is in lid 2 van artikel 11.2a van de Tw bijvoorbeeld een uitzondering geformuleerd voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder. Het artikel geeft echter op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens (maar uitzonderingen op het verwerkingsverbod).

Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.3 en/of artikel 11.2a van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Dat daargelaten, geeft de regeling in artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en (richtlijnconforme uitleg van)²⁷⁴ artikel

²⁷³ Te weten: het vereiste dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (beveiliging). Vgl. T&C Telecommunicatierecht, commentaar op artikel 11.3 Telecommunicatiewet en T&C Telecommunicatierecht, commentaar op artikel 13 WBP.

²⁷⁴ Een bepaling van een richtlijn die niet (volledig) tijdig en correct is omgezet, dient richtlijnconform te worden geïnterpreteerd. Zie o.a. HvJ EG 5 oktober 2004, gevoegde

5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) een nadere begrenzing/inperking van de toegestane verwerkingen van persoonsgegevens die ook communicatie betreffen in de telecommunicatiesector, namelijk waar het gaat om de vraag of daarvoor een grondslag is te vinden in de Wbp. Het CBP toetst de beoordeling van de grondslag voor het verwerken van persoonsgegevens die ook communicatie betreffen derhalve aan artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp. Dat betekent materieel (inhoudelijk) dat als de gegevensverwerking is toegestaan onder artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw; dat wil zeggen: uit dit artikel een wettelijke plicht voortvloeit) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw; dat wil zeggen: uit dit artikel een verwerkings-/uitzonderingsgrond voortvloeit) ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw ook geen grondslag is te vinden in de Wbp (waarbij dit laatste artikel 8 van de Wbp in de toets materieel (inhoudelijk) dan enkel zijdelings een rol speelt).

Beoordeling

3.6.1 Netwerkplanning en -beheer

Het CBP heeft in paragraaf 2.4 (p. 21 e.v. van dit rapport) vastgesteld dat KPN tot 21 september dan wel 11 oktober 2012 unieke klant- en toestelidentifiers in combinatie met gegevens over het bezoek aan en gebruik van apps en websites inspecteerde/genereerde, gebruikte, vastlegde en gedurende negentig dagen bewaarde voor netwerkplanning en -beheer (daaronder begrepen het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie en netwerkcapaciteitsplanning).

Het CBP heeft in de paragrafen 3.3 tot en met 3.5 (p. 49 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

KPN stelt in haar zienswijzen dat zij zich voor netwerkplanning en -beheer baseert op het verwerkingsdoeleinde verkeersbeheer.²⁷⁵ KPN voegt daar in haar zienswijze 2 aan toe dat uit de wetsgeschiedenis van artikel 11.2a van de Tw blijkt dat het telecommunicatieaanbieders al op grond van de huidige praktijk is toegestaan om voor goed netwerkbeheer te controleren welke applicaties en apparatuur worden gebruikt: dit artikel is een codificatie van de bestaande praktijk en beoogt dus geen wijzigingen door te voeren.²⁷⁶

Als hoofdregel geldt op grond van 11.2a van de Tw dat het af luisteren, aftappen, op slaan of anderszins onderscheppen of controleren van de communicatie én de

zaken C- 397/01 tot C-403/01 (*Pfeiffer*). KPN doet in haar zienswijze 2 een beroep op dit artikel als het gaat om de grondslag voor zover communicatie wordt verwerkt. Zienswijze 2 KPN, p. 33-43.

²⁷⁵ Zienswijze 1 KPN, p. 4; zie ook idem, p. 15-22 en 60. Zienswijze 2 KPN, p. 26-28.

²⁷⁶ Zienswijze 2 KPN, p. 38.

daarmee verband houdende verkeersgegevens door anderen dan de gebruikers verboden is, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit artikel geeft aldus een verwerkingsverbod, met uitzonderingen. Er is dus geen verplichting, opgenomen in een wettelijke bepaling, waarvan de gegevensverwerking een noodzakelijk uitvloeisel is. Op deze eerder genoemde hoofdregel is in lid 2 van artikel 11.2a van de Tw bijvoorbeeld een uitzondering geformuleerd voor het overbrengen van informatie via van de netwerken en diensten van de betrokken aanbieder. Uit de wetsgeschiedenis bij artikel 11.2a van de Tw volgt dat dit artikel er niet aan in de weg staat dat een aanbieder van een netwerk gegevens *verzamelt* over het volume van het verkeer van bepaalde diensten of applicaties, het aantal keren dat verbinding wordt gemaakt etc. om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is, mits het verzamelen van dergelijke gegevens niet verder gaat dan nodig is voor het goed laten functioneren van het netwerk en de daarover afgewikkelde diensten (proportionaliteitstoets). Het artikel geeft bovendien op zichzelf geen grondslag voor de *verwerking* van verkeersgegevens die ook persoonsgegevens zijn (maar uitzonderingen op het verwerkingsverbod). Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst met data-analyse technieken zulke gegevens wil verzamelen voor de in artikel 11.2a van de Tw genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Activiteiten tot behoud/verbetering van de netwerk performance of de dienstverlening van de mobiele aanbieder (waaronder netwerkplanning) *kunnen*, mede gelet op de wetsgeschiedenis bij artikel 11.2a van de Tw, in beginsel onder het verwerkingsdoel verkeersbeheer vallen (mits er een proportionele implementatie is).²⁷⁷

Ten aanzien van het inspecteren/genereren (verzamelen) van de persoonsgegevens geldt dat er voor KPN een noodzaak was om de gegevens op deze niet-geanonimiseerde wijze te verwerken om de benodigde informatie te hebben/(kunnen) krijgen (verzamelen) over de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps en websites. KPN heeft aannemelijk gemaakt dat er, gegeven de huidige stand van de techniek, geen andere manieren en minder ingrijpende middelen beschikbaar waren/zijn om hetzelfde resultaat te bereiken.

De noodzaak om gegevens over het dataverkeer te verzamelen behelst niet (zonder meer) een noodzaak om de aldus verkregen gegevens vervolgens ook op individueel persoonsniveau te gebruiken, vast te leggen en te bewaren. Getoetst moet worden of ook deze verwerking voldoet aan het proportionaliteits- en subsidiariteitsvereiste. De aard van de verzamelde persoonsgegevens, de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor gegevensvergaring in de vorm van data-analyse technieken naar aanleiding van het gebruik van het netwerk van de aanbieders en het risico (kans x impact) voor de betrokkenen van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, spelen een rol

²⁷⁷ Vgl. o.a. *Kamerstukken I* 2011/12, 32 549, E, p. 13 over het beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is de diverse verkeersstromen die over dat netwerk worden afgewikkeld in kaart brengen.

in de belangenafweging. Daarnaast worden de inspanning en kosten meegewogen die voor KPN gepaard gaan met de ontwikkeling en implementatie van (technische) mogelijkheden om hetzelfde doel op een andere, minder inbreukmakende wijze te bereiken, evenals de consequenties voor de continuïteit en integriteit van haar netwerk.

Ten aanzien van het gebruiken, vastleggen en gedurende negentig dagen bewaren van de persoonsgegevens geldt dat niet aannemelijk is dat KPN deze (zolang) in niet geanonimiseerde vorm moest/moet verwerken.

KPN legt in haar zienswijze uit dat de door het KPN [VERTROUWELIJK] voor netwerkplanning en -beheer verwerkte gegevens uitsluitend worden gebruikt voor kwantitatief statistisch en technisch onderzoek (trendanalyses).²⁷⁸ Te weten: (i) welk signaleringsverkeer en netwerkgebruik ontstaat door het gebruik van bepaalde apps, (ii) wat is de impact (waaronder het moment van impact) daarvan op specifieke onderdelen van het mobiele KPN netwerk en (iii) wat zijn de gedetailleerde ontwikkelingen ten aanzien van (i) en (ii).²⁷⁹

Het CBP oordeelt dat om zulke trends in gebruikersverkeer te identificeren voor netwerk(capaciteits)planning de persoonsgegevens (daarom) kunnen worden geaggregeerd naar gebruikersgroepniveau of netwerkelement en onomkeerbaar kunnen worden ontdaan van persoonsidentificerende kenmerken.

Het CBP verwijst hierbij (ook) naar overweging 30 van de e-Privacyrichtlijn dat activiteiten die verder gaan dan noodzakelijk voor de transmissie van communicatie en de facturering ervan moeten worden gebaseerd op geaggregeerde verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht én dat systemen voor elektronische-communicatienetwerken op dusdanige wijze moeten worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt.

Het CBP verwijst - nu de door het KPN [VERTROUWELIJK] voor netwerkplanning en -beheer verwerkte gegevens uitsluitend worden gebruikt voor kwantitatief statistisch en technisch onderzoek - verder naar een arrest van het Hof van Justitie van de EG van 16 december 2008, waaruit volgt dat indien het (enige) doel de vergaring van statistische gegevens is, het voor dat doeleinde niet noodzakelijk is om de gegevens op naam te bewaren en te verwerken.²⁸⁰

Er waren/zijn daarnaast meerdere mogelijkheden, en minder ingrijpende middelen, om hetzelfde resultaat te bereiken. Bijvoorbeeld, door (apparatuur die in staat is om) de persoonsgegevens zo snel mogelijk na het verzamelen onomkeerbaar te anonimiseren in niet-persistent (werk)geheugen. Technische mogelijkheden in dat verband zijn onder andere (i) het (laten) aanpassen van de configuratie-instellingen op bestaande data-analyse apparatuur, zodat de gegevens/persoonsidentificerende kenmerken direct na het verzamelen worden verwijderd uit de verkregen dataset, (ii)

²⁷⁸ Zienswijze 1 KPN, p. 49.

²⁷⁹ Idem, p. 51.

²⁸⁰ HvJ EG 16 december 2008, EHRC 2009, 23. (LJN BG7811; Huber).

het (doen) vervangen van bestaande data-analyse apparatuur door apparatuur die (wel) in staat is om de gegevens zo snel mogelijk na het verzamelen onomkeerbaar te anonimiseren (in niet-persistent (werk)geheugen) of (iii) het (laten) toevoegen van een zogeheten privacy filter (al dan niet op een ander of afzonderlijk apparaat) om de gegevens direct of zo snel mogelijk na het verzamelen onomkeerbaar te anonimiseren.²⁸¹

Het CBP heeft verder de consequenties in aanmerking genomen voor de continuïteit en integriteit van haar netwerk als KPN de benodigde gegevens niet kan verkrijgen over de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps en websites én de inspanningen en kosten voor KPN bij de ontwikkeling en implementatie van een alternatieve oplossing.

[VERTROUWELIJK]

KPN heeft in haar zienswijze 2 erkend dat deze gegevensverwerking niet proportioneel was, in de zin dat zij het invoeren van een technisch alternatief (anonimiseringsoplossing) die verkeersgegevens zo snel mogelijk onomkeerbaar anonimiseert op dit moment proportioneel acht.²⁸²

Uit het voorgaande volgt dat de door KPN gehanteerde wijze van verwerken van de persoonsgegevens in niet-geanonimiseerde vorm, na het verzamelen daarvan, niet noodzakelijk was voor verkeersbeheer.

Dat geldt temeer nu het herkennen/identificeren van het bezoek aan en gebruik van apps en websites kan leiden tot een omvangrijke verzameling van gevoelige persoonsgegevens die iets (kunnen) zeggen over het gedrag van mensen op internet. Deze gegevens raken aan de vertrouwelijke communicatie. Het enkele feit dat het daarbij niet gaat om het vastleggen en bewaren van individueel (historisch) surfgedrag (een reeks van volledige URL's van de webpagina's die een abonnee door de tijd heen bezoekt/heeft bezocht, waaruit bijvoorbeeld kan worden afgeleid hoe lang hij naar een bepaalde afbeelding of tekst heeft gekeken) maakt de hiervoor genoemde persoonsgegevens over het bezoek aan en gebruik van apps, websites op zich niet minder gevoelig. Ook hostnames (URL op hoofddomein) kunnen veel zeggen over de interesses, lifestyle, en eventueel gezondheid en/of seksuele voorkeur van de betrokken abonnee. De impact van oneigenlijk gebruik van de gegevens kan

²⁸¹ Het CBP merkt op dat KPN heeft verklaard: "KPN heeft als designrichtlijn om zo weinig mogelijk processing in te zetten, en zet daarom alleen zwaardere methoden in als dit niet anders mogelijk is." Bijlage 2 bij reactie KPN op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 3. Ter nadere onderbouwing wijst het CBP erop dat de hierboven gegeven voorbeelden van andere mogelijkheden en minder ingrijpende middelen een uitwerking vormen van de eisen van doelbinding en dataminimalisatie. Doelbinding betekent dat het doel waarvoor persoonsgegevens worden verzameld, bepalend is voor het verdere gebruik van deze gegevens. De persoonsgegevens mogen alleen voor gespecificeerde doelen worden verwerkt, de gegevens moeten noodzakelijk zijn voor het gestelde doel, en de verwerking moet verenigbaar zijn met dat doel. Dataminimalisatie betekent dat niet meer persoonsgegevens mogen worden verzameld en gebruikt dan strikt noodzakelijk is.

²⁸² Zienswijze 2 KPN, p. 2-5.

groot zijn. Daar komt bij dat het CBP heeft vastgesteld dat KPN (ook) referers (laatst bezochte website) verwerkte om websites/apps te herkennen/identificeren.

Daarbij leert de praktijk dat ondanks (passende) technische en organisatorische maatregelen om oneigenlijk gebruik van gegevens te voorkomen, (beveiligings)incidenten niet altijd kunnen worden voorkomen. Gelet op de aard van de verzamelde persoonsgegevens bieden andere maatregelen dan het direct na het verzamelen verwijderen van de persoonsgegevens uit de verkregen dataset, bijvoorbeeld door onomkeerbare anonimisering in niet-persistent (werk)geheugen, onvoldoende waarborgen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de betrokken abonnees.

Omdat KPN de persoonsgegevens die ook verkeersgegevens zijn voor verkeersbeheer niet direct na het verzamelen verwijderde terwijl dat wel mogelijk was, kon het zolang verwerken van de gegevens in niet-geanonimiseerde vorm niet als noodzakelijk worden beschouwd. Doordat de verwerking niet proportioneel en subsidiair was voor verkeersbeheer en omdat KPN ook geen ander noodzakelijk verwerkingsdoel had voor de onder dit kopje besproken gegevensverwerking, handelde KPN in strijd met artikel 11.5 van de Tw. Hierdoor kon van een grondslag als genoemd in artikel 8 van de Wbp evenmin sprake zijn en handelde KPN tevens in strijd met artikel 8 van de Wbp.

Getroffen maatregelen

Door het stopzetten en gestopt houden van de data-analysetool voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) alsmede de verwijdering van de verzamelde en verwerkte [VERTROUWELIJK: apparatuur]-gegevens, worden voor dit hiervoor genoemde doeleinde thans geen persoonsgegevens die ook verkeersgegevens zijn meer verwerkt en handelt KPN (daardoor) niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

Ten aanzien van door [VERTROUWELIJK] geoffreerde en door KPN voorgestelde anonimiseringsoplossing voor de data-analysetool voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) die KPN voornemens is te implementeren, geldt het volgende. In de oplossing worden (samengevat weergegeven) [VERTROUWELIJK] om op een minst ingrijpende manier voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer te kunnen komen tot statistisch betrouwbare analyses van trends in haar mobiele netwerk. Het CBP acht het aannemelijk dat het voor KPN noodzakelijk is om op basis van een zo groot mogelijke steekproef, gedurende 24 uur niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn te verwerken voor het doeleinde van netwerkplanning en -beheer om te kunnen komen tot statistisch betrouwbare analyses van (acute) trends in het mobiele netwerk. KPN verwacht de anonimiseringsoplossing op 1 juni 2013 te kunnen (laten) implementeren. [VERTROUWELIJK]. Op basis van het beschikbare onderzoeksmateriaal constateert het CBP, mits KPN op adequate wijze de risico's op (her)identificatie minimaliseert en doelbinding zeker stelt (wat zij heeft toegezegd), alsdan ten aanzien van de gegevensverwerking voor netwerkplanning en -beheer in

deze specifieke context via de door KPN voorgestelde anonimiseringsoplossing geen overtreding van artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).²⁸³

3.6.2 Prepaidverkeer

Het CBP heeft in paragraaf 2.5 (p. 34 e.v. van dit rapport) vastgesteld dat KPN tot 3 oktober 2012 (een) unieke klant- en/of toestelidentificatie(s), in combinatie met URL's inspecteerde en gebruikte om daaruit gratis opwaardeersites te herkennen voor het faciliteren van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed.

Het CBP heeft in de paragrafen 3.3. tot en met 3.5 (p. 49 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Zoals vermeld in de uitwerking van het wettelijk kader, geldt als hoofdregel op grond van artikel 11.5, eerste lid, van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer noodzakelijk zijn ten behoeve van (het doel van) de overbrenging van communicatie. Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor facturering). Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Als de gegevensverwerking is toegestaan onder artikel 11.5 van de Tw is ook een bijbehorende grondslag te vinden als opgesomd in artikel 8 van de Wbp (waarbij dit laatste artikel in de toets materieel (inhoudelijk) enkel zijdelings een rol speelt) en - omgekeerd - als de verwerking niet is toegestaan onder de Tw is ook geen grondslag te vinden in de Wbp.

Ten aanzien van (de toets van) het verwerkingsdoel facturering als bedoeld in artikel 11.5, tweede lid, van de Tw geldt het volgende.

KPN stelt in haar zienswijze dat zij zich voor het routeren van verkeer naar opwaardeersites voor opwaardering baseert op het verwerkingsdoel facturering.²⁸⁴ Dit verwerkingsdoel correspondeert - mogelijk - met de grondslagen uitvoering van een overeenkomst en/of noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

Uit de wetsgeschiedenis bij de Tw volgt dat het verwerkingsdoel facturering 'ruim' dient te worden opgevat in de zin dat verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die

²⁸³ Reactie KPN verzoek om inlichtingen van 6 en 15 februari 2013. Reactie KPN op vordering van 28 februari 2013.

²⁸⁴ Zienswijze 1 KPN, p. 64. Zienswijze 2 KPN, p. 60-66.

gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed (dit laatste dient onder facturering te worden begrepen).²⁸⁵

De enkele omstandigheid dat onder de verwerking ten behoeve van de facturering niet alleen wordt verstaan het opstellen van een factuur, maar ook het afwaarderen van het prepaidtegoed bij gebruik van de prepaidaansluiting met de verschuldigde vergoedingen en het bijhouden van het tegoed (het betreft immers vooruitbetaalde kaarten/gebruiksrechten, als het prepaidtegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante dienst (nog) te gebruiken²⁸⁶), maakt niet dat *het bieden van de mogelijkheid om nieuw tegoed te kopen* daar ook (zonder meer) onder valt. Uit een ontoereikend prepaidtegoed vloeit op zichzelf geen betalingsverplichting voort. Het prepaidtegoed is tenslotte al met de verschuldigde vergoedingen afgewaardeerd vanwege het gebruik van de prepaidaansluiting.²⁸⁷ Het faciliteren van opwaardeermogelijkheden is in beginsel - naar zijn aard - veeleer een verkoopactiviteit in de zin van artikel 11.5, derde lid, van de Tw waarvoor toestemming is vereist (die bij opwaardering een betalingsverplichting in het leven roept wat (wederom) noodzaakt tot het bijhouden van het tegoed).

Op grond van haar algemene voorwaarden 'Algemene voorwaarden en aanvullende voorwaarden voor mobiele telecommunicatiediensten 2012' heeft KPN (evenwel) een resultaatsverplichting om opwaardeermogelijkheden te bieden. Ofschoon uit deze algemene voorwaarden niet met zoveel woorden blijkt dat KPN zich heeft verbonden om bij een ontoereikend prepaid tegoed (ook) via 'mobiel internet' opwaardeermogelijkheden te bieden (om te voorkomen dat de betrokken abonnee zijn prepaidtegoed alsdan alleen kan opwaarderen via bijvoorbeeld een andere, 'vaste' internetverbinding), volgt hieruit dat de verwerking van gegevens om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor de facturering. Een abonnee verwacht dit ook.

Het CBP heeft deze uitleg van de wet, dat het faciliteren van opwaardeermogelijkheden op het eerste gezicht wellicht een verkoopactiviteit lijkt waarvoor toestemming is vereist, maar gelet op de resultaatsverplichting om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor het ruime verwerkingsdoel facturering, (nogmaals) voorgelegd aan het Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom - CBP. Het Agentschap Telecom stemt in met deze voorgelegde toepassing van dit wetsartikel.

Voor dit doeleinde verwerkte KPN (evenwel) ook gegevens van abonnees met een *postpaid* data abonnement en prepaid abonnees *met een toereikend tegoed*, omdat de

²⁸⁵ Kamerstukken II 2002/03, 28 851, nr. 13, p. 20.

²⁸⁶ Vgl. ook artikel 3:3, derde lid, van de Algemene voorwaarden en aanvullende voorwaarden voor mobiele telecommunicatiediensten 2012 Versie 30 juli 2012: "*KPN zal het relevante Prepaid-tegoed bij gebruik van de Prepaid-aansluiting afwaarderen met de verschuldigde vergoedingen. Als het Prepaid-tegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante Dienst te gebruiken en kan het gebruik van de Prepaid-aansluiting worden verbroken.*" URL: <http://www.kpn.com/allevoorwaarden.htm>.

²⁸⁷ Vgl. o.a. artikel 3:3 tot en met 3:5 van de Algemene voorwaarden en aanvullende voorwaarden voor mobiele telecommunicatiediensten 2012 Versie 30 juli 2012.

data-analyse technieken niet alleen zouden kunnen worden toegepast als een prepaid abonnee geen tegoed meer heeft (zie ook paragraaf 2.5, p. 34 e.v. van dit rapport). Hierdoor was de inbreuk op de belangen van deze betrokkenen onevenredig in verhouding tot het met de verwerking te dienen doel.

Verder zijn en waren er meerdere mogelijkheden, en minder ingrijpende middelen, om hetzelfde resultaat te bereiken, te weten: het er voor zorgen dat prepaid abonnees zonder tegoed toegang hebben tot (gratis) opwaardeersites om opwaarderen te faciliteren. Bijvoorbeeld, door een technisch alternatief te gebruiken, zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een betalingswebsite kan bezoeken.

Hieruit volgt dat de verwerkte gegevens niet noodzakelijk waren voor de facturering (proportionaliteitstoets). Nu van noodzaak voor facturering niet is gebleken en KPN ook geen ander mogelijk verwerkingsdoel had voor de in deze paragraaf besproken verwerking van persoonsgegevens, handelde KPN in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Getroffen maatregelen

Doordat KPN de inzet van de URL-detectiefunctie van de [VERTROUWELIJK: apparatuur] heeft gedeconfigureerd (waardoor deze niet meer beschikbaar is) en niet meer zal her-installeren, verleent KPN thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK]. Dit is in deze context een proportionele implementatie van het bieden van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed, direct via 'mobiel internet', gelet op de omstandigheid dat de verwerkte gegevens [VERTROUWELIJK] en niet worden opgeslagen en bewaard. Door deze aanpassing handelt KPN niet in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

3.6.3 Firewalls, spamfilters en virusscanners

Het CBP heeft in paragraaf 2.6 (p. 38 e.v. van dit rapport) vastgesteld dat KPN (een) unieke klant- en/of toestelidentificatie(s), in combinatie met spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer van betrokkenen inspecteert/verzamelt en gebruikt om beveiligings- en netwerkindegriteitsproblemen te voorkomen.

Het CBP heeft in de paragrafen 3.3. tot en met 3.5 (p. 49 e.v. van dit rapport) vastgesteld dat dit een verwerking van persoonsgegevens die ook communicatie betreffen is.

KPN heeft niet verklaard en uit het onderzoek is ook overigens niet gebleken dat de verwerking van persoonsgegevens voor dit doeleinde is gebaseerd op (ondubbelzinnige) toestemming (artikel 5, eerste lid, van de e-Privacyrichtlijn/artikel 11.2a, tweede lid, onder a, van de Tw jo. artikel 8, aanhef en onder a, van de Wbp).

Ten aanzien van (de toets van) de uitzonderingsgrond 'bij wet toegestaan' geldt het volgende. Deze uitzondering correspondeert - mogelijk - met de grondslagen uitvoering van een overeenkomst, wettelijke plicht en/of noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b, c en/of f, van de Wbp).

KPN heeft verklaard dat data-analyse technieken ten behoeve van het gebruik van firewalls, spamfilters en virusscanners (inclusief malware) noodzakelijk zijn, mede omdat anders binnen de internetgemeenschap de reputatie van het netwerk af zou nemen.²⁸⁸

Het CBP heeft in paragraaf 2.6 (p. 38 e.v. van dit rapport) vastgesteld dat internet aanbieders ook naar de inhoud van (gedownload) bestanden en verzonden en ontvangen e-mails moeten kijken om spam/virussen/malware te kunnen herkennen. Een alternatieve vorm van data-analyse waarbij bijvoorbeeld alleen naar headergegevens wordt gekeken, schiet tekort.

Artikel 11.3 van de Tw (de implementatie van artikel 4 van de e-Privacyrichtlijn) geeft een verplichting voor de aanbieder van een openbare elektronische communicatiedienst en -netwerk om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Onder de eisen die de zorgplicht internetveiligheid stelt, kan naar het oordeel van het CBP ook het aanbieden van virusfilters voor inkomende en eventueel uitgaande e-mails worden begrepen en het bestrijden van spyware.²⁸⁹

Hieruit volgt dat de verwerking van de spam- (bij uitgaande spam), virus- en malwareherkenningsgegevens noodzakelijk is voor (de uitvoering van) de zorgplicht internetveiligheid.²⁹⁰

Uit het voorgaande blijkt dat KPN een grondslag voor deze verwerking van persoonsgegevens die ook communicatie betreffen, heeft onder artikel 11.3 van de Tw jo. artikel 8 van de Wbp. Op basis van het beschikbare onderzoeksmateriaal heeft het CBP ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens die ook communicatie betreffen geen overtreding geconstateerd van artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp.

Op grond van de 'Aanvullende Voorwaarden voor gebruik van het mobiel netwerk van KPN voor datadiensten' heeft KPN een inspanningsverplichting om verspreiding van ongevraagde e-mail gericht aan haar gebruikers (inkomende spam) te beperken.²⁹¹

Op 1 januari 2013 is artikel 7.4a van de Tw inwerking getreden. Artikel 7.4a, eerste lid, aanhef en onder c, van de Tw regelt een toestemmingsvereiste voor het filteren op inkomende spam. In de wetsgeschiedenis bij de Tw is daarover opgemerkt: *"Daarnaast kan het generiek filteren van inkomende spam nuttig zijn omdat klanten dit op prijs stellen en*

²⁸⁸ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 4-5.

²⁸⁹ In de opinie van de Artikel 29-werkgroep is in 2006 opgemerkt dat filtering van (inkomende) spam onder omstandigheden kan worden gebaseerd op de grondslag uitvoering van een overeenkomst en/of wettelijke plicht (vgl. artikel 8, aanhef en onder b en c, van de Wbp). WP118 Advies 2/2006 over de privacyaspecten van e-mailscreeningdiensten, p. 6.

²⁹⁰ Aanvullende Voorwaarden voor gebruik van het mobiel netwerk van KPN voor datadiensten (geldig vanaf 5 september 2011).

²⁹¹ Privacy - Hi.

omdat het onnodige belasting van netwerken en systemen voorkomt. Artikel 7.4a, eerste lid, onderdeel c, stelt hiervoor wel als voorwaarde dat de abonnee toestemming heeft gegeven. De aanbieder die alleen generiek op spam wil filteren, zou ervoor kunnen kiezen om bij het afsluiten van een overeenkomst te wijzen op het nut van een spamfilter en het geven van toestemming als voorwaarde voor het sluiten van de overeenkomst te stellen.”²⁹²

Het Samenwerkingsprotocol CBP-OPTA (zijnde werkafspraken tussen de verschillende toezichthouders binnen de grenzen van de onderscheidene wetten waarin hun bevoegdheden zijn geregeld) regelt/geeft onder andere bepalingen over de behandeling bij samenlopende bevoegdheden en de uitwisseling en verstrekking van informatie tussen de ACM²⁹³ en het CBP. Op grond van artikel 2, tweede en derde lid, van het Samenwerkingsprotocol CBP-OPTA zal de ACM zich bij het uitoefenen van haar bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van de bepalingen van de Tw ligt en zal het CBP zich bij het uitoefenen van zijn bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van bepalingen van de Wbp ligt. Het beoordelen van (de toelaatbaarheid van) het filteren op inkomende spam ligt volgens de toezichthouders vanaf de inwerkingtreding van artikel 7.4a van de Tw meer op de weg van de ACM.²⁹⁴ De inzet van data-analyse technieken vanaf 1 januari 2013 voor het filteren op inkomende spam valt daarom buiten de scope van dit onderzoek.

3.6.4 Behandeling van klantklachten

Het CBP heeft in paragraaf 2.7 (p. 41 e.v. van dit rapport) vastgesteld dat KPN gegevens over (en voor zover het voor de behandeling van een klantklacht noodzakelijk is om dit te openen, ook uit) het dataverkeer van betrokkenen inspecteert/verzamelt, gebruikt en - als ook offline analyse noodzakelijk is²⁹⁵ - vastlegt om technische incidenten en klantproblemen op te lossen in individuele gevallen.²⁹⁶

Het CBP heeft in de paragrafen 3.3. tot en met 3.5 (p. 49 e.v. van dit rapport) vastgesteld dat dit een verwerking van persoonsgegevens (tevens verkeersgegevens respectievelijk communicatie) is.

KPN heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming.

Persoonsgegevens die ook verkeersgegevens zijn

Ten aanzien van (de toets van) het verwerkingsdoel behandeling van verzoeken om inlichtingen van klanten geldt het volgende.

²⁹² Kamerstukken I 2011/12, 32 549, G, p. 8.

²⁹³ De ACM is krachtens artikel 42, zesde lid, van de Instellingswet Autoriteit Consument en Markt in dit Samenwerkingsprotocol CBP-OPTA per [1 april 2013] in de plaats getreden van OPTA.

²⁹⁴ Vgl. ook de taakverdeling ten aanzien van spam (artikel 5 van het Samenwerkingsprotocol CBP-OPTA). Het artikel geeft op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens, maar uitzonderingen op het verwerkingsverbod.

²⁹⁵ Reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

²⁹⁶ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 2.

KPN heeft als verzamel- en verwerkingsdoeleinde van de persoonsgegevens genoemd 'de behandeling van klantklachten (dat wil zeggen: het oplossen van technische incidenten en klantproblemen in individuele gevallen)'. Uit het voorgaande blijkt dat KPN (daarom) een grondslag voor deze verwerking van persoonsgegevens die ook verkeersgegevens zijn zou kunnen hebben onder artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw. Zo'n verwerkingsdoel correspondeert - mogelijk - met de grondslagen uitvoering van een overeenkomst en/of noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

Op basis van het beschikbare onderzoeksmateriaal heeft het CBP ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens die ook verkeersgegevens zijn geen overtreding geconstateerd van artikel 11.5 van de Tw jo artikel 8 van de Wbp.

Persoonsgegevens die ook communicatie betreffen

KPN heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming. Voor zover KPN betrokkenen om voorafgaande ondubbelzinnige toestemming vraagt (dat wil zeggen: voorafgaand aan de gegevensverzameling) en die toestemming wordt verkregen, correspondeert dit met de uitzonderingsgrond/grondslag (ondubbelzinnige) toestemming (artikel 5, eerste lid, van de e-Privacyrichtlijn/artikel 11.2a, tweede lid, onder a, van de Tw jo. artikel 8, aanhef en onder a, van de Wbp).

Indien en voor zover KPN zou claimen dat ondubbelzinnige toestemming is/wordt verkregen via het Privacy Statement, wijst het CBP erop dat van toestemming slechts sprake is indien deze 'vrij', 'specifiek' en 'geïnformeerd' is. 'Specifiek' betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging). 'Ondubbelzinnig' betekent dat bij de verantwoordelijke elke twijfel moet zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven (zie p. 70 van dit rapport). In de wetsgeschiedenis bij de Wbp is in dat verband 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."*²⁹⁷ Hieruit volgt dat ondubbelzinnige toestemming niet via het Privacy Statement kan worden verkregen.

Op basis van het beschikbare onderzoeksmateriaal heeft het CBP ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens die ook communicatie betreffen geen overtreding geconstateerd van artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp.

Getroffen maatregelen

KPN geeft in haar zienswijze aan voornemens te zijn (ook) een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-omgeving in te richten om - ondanks de

²⁹⁷ *Handelingen I* 1999/2000, 34, p. 1632.

anonymiseringsoplossing - klantklachten over te hoge rekeningen op te kunnen lossen.²⁹⁸ De (mogelijke) inzet van data-analyse technieken voor de behandeling van klantklachten via een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-omgeving in de toekomst valt buiten de scope van dit onderzoek.

3.6.5 Verdere verwerking

KPN heeft in april 2011 voor marktonderzoek (analyse van de eigen dienstverlening) per abonnee geaggregeerde persoonsgegevens die ook tevens verkeersgegevens zijn (inclusief de unieke IMSI-klantnummers van betrokkenen)²⁹⁹ over het gebruik van WhatsApp aan het KPN retailbedrijf verstrekt.

KPN verstrekke sinds 29 juli 2011 tot september 2012 periodiek gegevens, niet zijnde persoonsgegevens, over het gebruik door al haar abonnees van een (groot) aantal apps en websites aan het KPN retailbedrijf voor marktonderzoek, maar pas nadat deze gegevens onomkeerbaar waren geanonimiseerd.

Het CBP heeft vastgesteld dat het KPN retailbedrijf vooral inzicht wilde hebben/krijgen in het gebruik van WhatsApp door Hi klanten (als 'early adopters').³⁰⁰

In het oude Privacy Statement van KPN en de oude privacyverklaring van Hi werd over het gebruik van verkeersgegevens voor marketing- en marktonderzoekdoeleinden opgemerkt dat dit (uitsluitend) plaatsvindt met toestemming: *"Ook je verkeersgegevens kunnen door KPN gebruikt worden voor marketingdoeleinden en voor het doen van aanbiedingen, maar uitsluitend voor zover je daarvoor vooraf je toestemming hebt gegeven. (...)."*³⁰¹ En: *"Wij verwerken je verkeersgegevens (zoals het tijdstip en de duur van het gebruik van een aansluiting, surfgedrag, kijkgedrag, IP-adressen en URL's) voor de volgende doeleinden: (...) f. Ten behoeve van marktonderzoek en verkoopactiviteiten voor producten en diensten van Hi, ook na beëindiging van het contract, mits je daarvoor toestemming hebt gegeven",* (onderstreping toegevoegd door het CBP).³⁰² Uit artikel 11.5, derde lid, van de Tw volgt dat verkeersgegevens alleen mogen worden verwerkt voor marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten als de betrokkene daarvoor zijn toestemming heeft gegeven. Zo'n verwerkingsdoel correspondeert - mogelijk - met de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp).

KPN heeft niet verklaard en uit het onderzoek is ook overigens niet gebleken dat KPN daadwerkelijk om (ondubbelzinnige) toestemming heeft gevraagd en die toestemming is verkregen.

Doordat KPN zonder ondubbelzinnige toestemming eenmalig persoonsgegevens (tevens verkeersgegevens) over het WhatsApp-gebruik (over de periode februari-april 2011) van alle KPN abonnees met een (postpaid of prepaid) data abonnement heeft

²⁹⁸ Zie o.a. reactie KPN op vordering van 28 februari 2013, p. 1.

²⁹⁹ Over de periode februari-april 2011. Bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

³⁰⁰ Reactie KPN op verzoek om inlichtingen van 1 september 2011, p. 3; bijlage 3 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011, p. 4.

³⁰¹ KPN Privacy Statement Januari 2011.

³⁰² Privacy - Hi.

verstrekt aan het KPN retailbedrijf, heeft zij in strijd gehandeld met artikel 11.5, derde lid, van de Tw jo. artikel 8 van de Wbp.

Ten aanzien van de periodieke verstrekking aan het KPN retailbedrijf van de onomkeerbaar geanonimiseerde gegevens over het gebruik door al haar abonnees van een (groot) aantal apps en websites, geldt dat het CBP in paragraaf 3.6.1 (p. 76 e.v. van dit rapport) heeft vastgesteld dat het inspecteren/genereren, gebruiken, vastleggen en bewaren van de persoonsgegevens door KPN voor netwerkplanning en -beheer onrechtmatig was, bij gebreke van een grondslag in de zin van artikel 11.5 van de Tw jo. artikel 8 van de Wbp. Nu KPN niet mocht beschikken over de initiële (achterliggende) persoonsgegevens, was het KPN ook niet toegestaan om deze gegevens naderhand te anonimiseren (te weten: een verwerking van persoonsgegevens) om ze (in geanonimiseerde vorm) verder te verwerken voor marktonderzoek.³⁰³ KPN heeft (daardoor) in strijd gehandeld met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Getroffen maatregelen

Doordat KPN de voor netwerkplanning en -beheer opgeslagen gegevens én de geanonimiseerde gegevens die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening per uiterlijk 11 oktober 2012 heeft verwijderd, handelt KPN niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

³⁰³ Dit onverminderd artikel 11.5, derde lid, van de Tw.

3.7 Uitdrukkelijk omschreven en gerechtvaardigde doeleinden

Persoonsgegevens mogen op grond van artikel 7 van de Wbp slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.

Uitwerking van het wettelijk kader

Artikel 7 van de Wbp bepaalt: *Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.*

‘Welbepaald en uitdrukkelijk omschreven’ betekent dat men geen gegevens mag verzamelen zonder een precieze doelomschrijving.³⁰⁴

‘Welbepaald’ houdt in dat de doelomschrijving duidelijk moet zijn (niet zo vaag of ruim dat deze tijdens het verzamelproces geen kader kan bieden waaraan kan worden getoetst of de gegevens nodig zijn voor dat doeleinde of niet).³⁰⁵ Het doeleinde mag ook niet in de loop van het verzamelproces worden geformuleerd.³⁰⁶ ‘Uitdrukkelijk omschreven’ houdt in dat de verantwoordelijke de doeleinden waarvoor hij persoonsgegevens verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 van de Wbp (hierna: de meldingsplicht) verplicht is te doen.³⁰⁷

Uit de wetsgeschiedenis blijkt dat van ‘gerechtvaardigde doeleinden’ alleen sprake kan zijn als deze met inachtneming van artikel 8 van de Wbp (grondslag) kunnen worden bereikt. *"De realisering van deze doeleinden zal in alle stadia van de gegevensverwerking moeten kunnen steunen op één of meer van de in artikel 8 genoemde gronden voor gegevensverwerking. Indien bijvoorbeeld een doel alleen bereikbaar is als persoonsgegevens in strijd met artikel 8 worden bewaard of aan een derde verstrekt, is niet voldaan aan het vereiste van een 'gerechtvaardigd doel' en mogen de betrokken gegevens op grond van artikel 7 ook niet worden verzameld."*³⁰⁸

De gegevensverwerking moet dus in alle stadia kunnen steunen op een of meer van de in artikel 8 van de Wbp genoemde gronden.

Beoordeling

Het CBP heeft in de paragrafen 2.4 tot en met 2.7 (p. 21 e.v. van dit rapport) vastgesteld dat KPN persoonsgegevens verzamelt/verwerkt bij de inzet van data-analyse technieken in haar mobiele netwerk.

KPN heeft als doeleinden van de gegevensverwerking geformuleerd, voor zover deze binnen de scope van dit onderzoek vallen: netwerkplanning en -beheer (daaronder mede begrepen het voorkomen van congestie en netwerkcapaciteitsplanning), het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed, het gebruik van firewalls, spamfilters en virusscanners

³⁰⁴ Kamerstukken II 1997/98, 25 892, nr. 3, p. 79.

³⁰⁵ Idem.

³⁰⁶ Idem.

³⁰⁷ Idem.

³⁰⁸ Idem.

(netwerkindegriteit en -continuïteit) en de behandeling van klantklachten. De twee doeleinden het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed en het gebruik van firewalls, spamfilters en virusscanners waren onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving in de (oude) melding die KPN bij het CBP had gedaan.

Het CBP heeft in paragraaf 2.1 (p. 15 van dit rapport) vastgesteld dat KPN geen andere meldingen had gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele netwerk. De in deze paragraaf bedoelde verwerkingen van persoonsgegevens voldoen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens niet aan de eisen die worden gesteld aan de categorieën van vrijgestelde verwerkingen die zijn beschreven in de artikelen van het Vrijstellingsbesluit Wbp.³⁰⁹ De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding.³¹⁰ KPN heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp, waardoor de meldingen bij die functionaris zouden kunnen zijn gedaan (artikel 27, derde lid, van de Wbp).

Doordat KPN de hiervoor genoemde twee doeleinden waarvoor zij persoonsgegevens verwerkt(e) onvolledig en onvoldoende duidelijk had omschreven bij de melding die zij bij het CBP had gedaan, werden de door KPN verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelde KPN in strijd met artikel 7 van de Wbp.

Het CBP heeft in de paragrafen 3.6.1 en 3.6.2 (p. 76 e.v. van dit rapport) vastgesteld dat KPN niet in alle stadia van de verwerking een grondslag had voor de gegevensverwerkingen voor de doeleinden netwerkplanning en -beheer en prepaidverkeer.

Doordat de gegevensverwerking voor de doeleinden netwerkplanning en -beheer en prepaidverkeer niet in alle stadia kon steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, werden de door KPN verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelde KPN in strijd met artikel 7 van de Wbp.

³⁰⁹ De enige artikelen die mogelijksterwijs in aanmerking zouden kunnen komen qua categorie(en) van vrijgestelde verwerking(en) zijn artikel 32 en 34 van het Vrijstellingsbesluit Wbp. Artikel 32 en 34 van het Vrijstellingsbesluit Wbp regelt slechts een vrijstelling van de melding voor verwerkingen in verband met het aanbieden van faciliteiten of diensten op een netwerk (niet zijnde een 'openbare elektronisch communicatienetwerk' of 'openbare elektronische communicatiediensten' als bedoeld in artikel 1.1, onder g en f, van de Tw) respectievelijk verwerkingen in verband met het gebruik van communicatieapparatuur die beschikbaar wordt gesteld 'aan personen die in dienst zijn van of werkzaam zijn ten behoeve van de verantwoordelijke', en dan nog alleen maar voor zover deze verwerkingen voldoen aan de in die artikelen vermelde eisen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens.

³¹⁰ Artikel 2 van het Vrijstellingsbesluit Wbp bepaalt: "*Artikel 27 van de wet [te weten: de Wbp; toevoeging door het CBP] is niet van toepassing op de in hoofdstuk 2 van dit besluit bedoelde verwerkingen van persoonsgegevens door of ten behoeve van één verantwoordelijke.*"

Getroffen maatregelen

KPN heeft de melding met nummer m1321211 op 9 maart 2012 gewijzigd (versienummer 4.0) (zie p. 16 e.v. van dit rapport).

Uit het voorgaande blijkt dat het doeleinde het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid en het gebruik van firewalls, spamfilters en virusscanners (netwerkindegriteit en -continuïteit) alsnog is omschreven bij de gewijzigde melding die KPN heeft gedaan.

Door het stopzetten en gestopt houden van de data-analysetool voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) en doordat KPN de inzet van de URL-detectiefunctie van de [VERTROUWELIJK: apparatuur] heeft gedeconfigureerd (waardoor deze niet meer beschikbaar is) en niet meer zal her-installeren, handelt KPN niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag) en zijn ook de overige door het CBP geconstateerde overtredingen van artikel 7 van de Wbp beëindigd.

3.8 Informatieplicht

Uitwerking van het wettelijk kader

Op grond van artikel 11.5, vierde lid, van de Tw stelt de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst de abonnee of gebruiker in kennis van de soorten verkeersgegevens die worden verwerkt ten behoeve van facturering, marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, en de levering van diensten met toegevoegde waarde alsmede omtrent de duur van de verwerking. Voor zover het de verwerking van verkeersgegevens ten behoeve van marktonderzoek of verkoopactiviteiten dan wel de levering van toegevoegde waardediensten betreft, wordt de desbetreffende informatie verstrekt voorafgaand aan het verkrijgen van de daarvoor benodigde toestemming van de abonnee of gebruiker.³¹¹

Aanvullend bepaalt artikel 34, eerste en tweede lid, van de Wbp dat 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

³¹¹ Aanvullend bepaalt artikel 11.2a, derde lid, van de Tw, (kort gezegd): *voorafgaand aan het verkrijgen van uitdrukkelijke toestemming* voor het aftappen, af luisteren of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende gegevens via een openbaar elektronisch communicatienetwerk of -dienst, verstrekt de aanbieder aan de abonnee de volgende informatie:

a. de soort gegevens die wordt afgetapt, afgeluisterd, onderschept of gecontroleerd;
b. de doeleinden waarvoor de gegevens worden afgetapt, afgeluisterd, onderschept of gecontroleerd, en
c. de duur van het aftappen, af luisteren, onderscheppen of controleren van de gegevens. Deze informatieplicht is in dit geval niet relevant omdat de toestemmingsuitzondering op het verwerkingsverbod van artikel 11.2a, tweede lid, onder a van de Tw niet aan de orde is.

b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

Artikel 34 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.³¹²

Deze bepaling vormt een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing'.³¹³ 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.³¹⁴ De betrokkene is in staat te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.³¹⁵

Artikel 34 van de Wbp gaat er vanuit dat er geen onderzoeksplicht van de betrokkene is.³¹⁶

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 34, derde jo. eerste lid, van de Wbp).

De hierboven beschreven (nadere) informatieplicht geldt niet indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning vergt. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast (artikel 34, vierde lid, van de Wbp).

De (nadere) informatieplicht geldt evenmin indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid (artikel 34, vijfde lid, van de Wbp).

Dit alles betekent dat wat betreft het factureringsdoel én voor zover de verwerkingsdoelen verkeersbeheer, opsporing van fraude en behandeling van verzoeken om inlichtingen van abonnees zijn afgeleid van het factureringsdoel, de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst de abonnee of gebruiker in kennis stelt van de soorten (categorieën) verkeersgegevens die worden verwerkt voor deze verwerkingsdoelen, alsmede omtrent de duur van de verwerking.

³¹² *Kamerstukken II 1997/98, 25 892, nr. 3, p. 149-150.*

³¹³ *Idem*, p. 149.

³¹⁴ *Idem*.

³¹⁵ *Idem*. De omstandigheid dat de informatieplicht een uitwerking vormt van het 'fair processing' beginsel uit artikel 6 van de Wbp heeft tot gevolg, dat overtreding van de informatieplicht zal leiden tot onrechtmatige verwerking(en). *Idem*.

³¹⁶ *Idem*, p. 150.

Aanvullend geldt de informatieplicht uit artikel 34 van de Wbp, voor zover het gaat om de verwerking van telecommunicatiegegevens die ook persoonsgegevens zijn.

Beoordeling

Het CBP heeft in de paragrafen 2.4 tot en met 2.7 (p. 21 e.v. van dit rapport) vastgesteld dat KPN persoonsgegevens die ook verkeersgegevens zijn verwerkt(e) voor de doeleinden netwerkplanning- en beheer (daaronder mede begrepen het voorkomen van congestie en netwerkcapaciteitsplanning), het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed en de behandeling van klantklachten.

Het CBP heeft in paragraaf 3.5 (p. 63 e.v. van dit rapport) vastgesteld dat KPN de persoonsgegevens die verkeersgegevens zijn, verzamelt/verzamelde met behulp van data-analyse apparatuur in haar mobiele netwerk. De persoonsgegevens worden/werden (aldus) verkregen op een andere wijze dan bij de betrokkene.

Hetzelfde geldt voor spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer. Het CBP heeft in paragraaf 2.6 (p. 38 e.v. van dit rapport) vastgesteld dat KPN deze persoonsgegevens die ook communicatie betreffen verwerkt(e) voor het doeleinde het gebruik van firewalls, spamfilters en virusscanners (netwerkindegriteit en -continuïteit).

Het CBP heeft in paragrafen 3.3 en 3.4 (p. 49 e.v. van dit rapport) vastgesteld dat de persoonsgegevens over het communicatiegedrag van betrokkenen gegevens van gevoelige aard zijn.

Wat betreft het factureringsdoel én voor zover de verwerkingsdoelen verkeersbeheer, opsporing van fraude en behandeling van verzoeken om inlichtingen van abonnees zijn afgeleid van het factureringsdoel, moet KPN betrokkenen in kennis stellen van de soorten (categorieën) verkeersgegevens die worden verwerkt voor deze verwerkingsdoelen, alsmede omtrent de duur van de verwerking. Aanvullend geldt de informatieplicht uit artikel 34 van de Wbp, voor zover het gaat om de verwerking van telecommunicatiegegevens die ook persoonsgegevens zijn, dat KPN de betrokkenen onder andere de doeleinden van de verwerking moet mededelen en nadere informatie verstrekt 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.

In het oude Privacy Statement van KPN werd (ten eerste) over het vastleggen/bijhouden van surfgedrag opgemerkt: *“Je surfgedrag wordt niet opgeslagen. KPN houdt niet bij welke websites je bezoekt. (...) KPN neemt geen kennis van de inhoud van je e-mailberichten. KPN neemt evenmin kennis van de inhoud van je chatberichten.”*³¹⁷

De persoonsgegevens (waaronder hostnames en referers) die ook verkeersgegevens zijn werden tot 21 september dan wel 11 oktober 2012 voor het doeleinde netwerkplanning en -beheer door KPN geïnspecteerd/gegenereerd, gebruikt, vastgelegd en bewaard op individueel persoonsniveau, althans

³¹⁷ Privacy Statement Januari 2011.

geaggregeerd per abonnee. Hieruit volgt dat de zinsnede in het oude Privacy Statement dat KPN 'niet bijhoudt welke websites worden bezocht' als feitelijk onjuist moet worden aangemerkt, althans onvolledig en onvoldoende duidelijk is. Dit terwijl de ratio van de informatieplicht is dat de burger in staat moet zijn te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.³¹⁸

KPN informeerde betrokkenen in het oude Privacy Statement van KPN, de oude privacyverklaring van Hi, de 'Algemene Voorwaarden voor mobiele telecommunicatiediensten' en de 'Aanvullende Voorwaarden voor gebruik van het mobiel netwerk van KPN voor datadiensten' (verder) niet over de doeleinden van de gegevensverwerking. Oftewel, niet over de verwerking van persoonsgegevens (waaronder URL's) 'voor het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed' en 'voor netwerkplanning en -beheer', waaronder verstaan: het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie' en over de duur van de verwerking (zie p. 31 e.v en p. 36 e.v. van dit rapport). KPN informeerde wel over het gebruik van firewalls, spamfilters en virusscanners voor netwerkintegriteit en -continuïteit en de behandeling van klantklachten.

Ten aanzien van de aanvullende werking van artikel 34 van de Wbp merkt het CBP verder nog het volgende op.

Gelet op de gevoelige aard van de persoonsgegevens, de omstandigheden waaronder de persoonsgegevens worden/werden verkregen (te weten: dat onopgemerkt gegevens omtrent betrokkenen worden/werden vergaard en verwerkt, met behulp van automatische procedures voor gegevensvergaring³¹⁹ in de vorm van data-analyse technieken) en het gebruik dat ervan wordt/werd gemaakt, is het nodig dat KPN de betrokkenen nadere informatie verstrekt(e) over de categorieën van verwerkte gegevens³²⁰ en de bewaartermijn om tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen.³²¹

Mededeling van de informatie aan de betrokkenen via een privacyverklaring/algemene voorwaarden op de KPN website is/was mogelijk en vergt geen onevenredige inspanning.

Het CBP heeft in paragraaf paragraaf 3.6.1 (p. 76 e.v. van dit rapport) vastgesteld dat de *vastlegging* van de persoonsgegevens niet bij of krachtens de wet is/was voorgeschreven.

Doordat KPN de betrokkenen niet uiterlijk op het moment van vastlegging van de hen betreffende persoonsgegevens meedeelde dat de gegevens worden/werden verwerkt

³¹⁸ *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 149.

³¹⁹ Vgl. *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 78.

³²⁰ Vgl. ook artikel 11, eerste lid, onder c, van de Privacyrichtlijn.

³²¹ Vgl. Last onder dwangsom NS Groep N.V. CBP 9 juni 2011, z2011-00057. URL: http://www.cbpreweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_NS.pdf (URL laatst bezocht op 29 mei 2013).

‘voor netwerkplanning en -beheer’, waaronder verstaan: het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie, en ‘voor het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed’ en omdat zij hen niet informeerde over de categorieën van verwerkte persoonsgegevens voor de doeleinden netwerkplanning en -beheer, de behandeling van klantklachten en de bewaartermijn, handelde KPN in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

Getroffen maatregel

Per eind mei 2012 heeft KPN het oude Privacy Statement van KPN en de oude privacyverklaring van Hi op deze punten aangevuld en gepreciseerd (zie p. 32 e.v. van dit rapport).

KPN heeft de doeleinden van de verwerking ‘voor netwerkplanning en -beheer’, waaronder verstaan: het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie, en ‘voor het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed’ en de categorieën van verwerkte persoonsgegevens, tevens verkeersgegevens alsnog beschreven in haar nieuwe privacy statements.

Hierdoor handelt KPN niet langer in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

3.9 Meldingsplicht

Uitwerking van het wettelijk kader

Artikel 27, eerste en derde lid, van de Wbp bepaalt: *een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, wordt alvorens met de verwerking wordt aangevangen gemeld bij het College of de functionaris.*

De melding behelst onder andere een opgave van het doel of de doeleinden van de verwerking, het doel of de doeleinden waarvoor de gegevens of de categorieën van gegevens zijn of worden verzameld en een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben (artikel 28, eerste en tweede lid, van de Wbp).

Beoordeling

Het CBP heeft in paragraaf 3.7 (p. 89 e.v. van dit rapport) vastgesteld dat KPN de doeleinden - samengevat weergegeven - het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeerwebsites bij een ontoereikend prepaid tegoed en het gebruik van firewalls, spamfilters en virusscanners (netwerkimintegriteit en – continuïteit) waarvoor zij persoonsgegevens verwerkt niet, althans onvolledig en onvoldoende duidelijk had omschreven bij de melding met nummer m1321211 (versienummer 3.0) die KPN op 3 september 2010 heeft gedaan.

Het CBP heeft in paragraaf 2.1 (p. 15 e.v. van dit rapport) vastgesteld dat KPN geen andere meldingen had gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele

netwerk. De verwerkingen van persoonsgegevens door KPN voor de hierboven genoemde doeleinden voldoen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens niet aan de eisen die worden gesteld aan de categorieën van vrijgestelde verwerkingen die zijn beschreven in de artikelen van het Vrijstellingsbesluit Wbp. De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding. KPN heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.

Doordat KPN deze verwerkingen van persoonsgegevens niet heeft gemeld bij het CBP, handelde KPN in strijd met artikel 27 jo. 28 van de Wbp.

Getroffen maatregelen

Het doeleinde het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid en het gebruik van firewalls, spamfilters en virusscanners (netwerkintegriteit en -continuïteit) zijn alsnog omschreven bij de gewijzigde melding die KPN heeft gedaan. Daardoor handelt KPN niet langer in strijd met artikel 27 jo. 28 van de Wbp.

3.10 Behoorlijk en zorgvuldig verwerken van persoonsgegevens

Uitwerking van het wettelijk kader

Artikel 6 van de Wbp bepaalt: *Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt*

Artikel 6 van de Wbp brengt tot uitdrukking dat geen gegevensverwerking mogelijk is die niet in overeenstemming is met de wet.

Artikel 6 keert zich onder meer tegen die vormen van gegevensverwerking die naar Angelsaksische traditie als 'unfair' of 'oneerlijk' worden beschouwd. Voorwaarde voor een eerlijke verwerking van gegevens is - zo stelt overweging 38 bij de Privacyrichtlijn - dat de betrokkenen van het bestaan van de verwerkingen kennis kunnen hebben en, wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze gegevens worden verkregen. Praktijken waarbij bij voorbeeld onopgemerkt gegevens omtrent personen worden vergaard en verwerkt, al dan niet met behulp van technische hulpmiddelen, zijn dus ongeoorloofd.³²²

Beoordeling

In het oude Privacy Statement van KPN en de oude privacyverklaring van Hi werd over het gebruik van verkeersgegevens voor marktonderzoek- en marketingdoeleinden opgemerkt dat dit (uitsluitend) plaatsvindt met toestemming. KPN heeft eenmalig (over de periode februari-april 2011), zonder (ondubbelzinnige) toestemming van de betrokkenen, op individueel abonneeniveau (dat wil zeggen: in combinatie met de unieke IMSI-klantnummers) aan het KPN retailbedrijf gegevens verstrekt voor marktonderzoek (analyse van de eigen dienstverlening) over het WhatsApp-gebruik van al haar abonnees (niet zijnde: alleen de voor de nadere analyse benodigde groep Hi klanten). Dat vormt een disproportionele inbreuk op de persoonlijke levenssfeer en was dus niet behoorlijk en niet zorgvuldig. KPN heeft daarom ten aanzien van deze gegevensverwerkingen gehandeld in strijd met artikel 6 van de Wbp. Doordat dit eenmalig was en KPN de gegevens die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening per uiterlijk 11 oktober 2012 heeft verwijderd, handelt KPN niet langer in strijd met artikel 6 van de Wbp.

³²² *Kamerstukken II 1997/98, 25 892, nr. 3, p. 78.*

4. CONCLUSIES

KPN past data-analyse technieken toe op het data- en signaleringsverkeer in haar mobiele netwerk.

Circa 3,8 miljoen KPN abonnees met een (prepaid of postpaid) data abonnement maken gebruik van dataverkeersdiensten van KPN.

KPN verwerkt(e) gegevens over en uit het dataverkeer van deze abonnees. Het gaat om (een) unieke klant- en/of toestel identifier(s) in combinatie met:

- gegevens over het bezoek aan en gebruik van apps en websites, tot 21 september 2012 dan wel 11 oktober 2012
- URL's om daaraan gratis opwaardeersites te herkennen, tot 3 oktober 2012
- spam-, virus- en malwareherkenningsgegevens uit (gedownload) bestanden en verzonden en ontvangen e-mails
- (technische) gegevens over het functioneren van het netwerk/toestel om een verzoek om inlichtingen af te handelen

Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn. De persoonsgegevens worden/werden door KPN verwerkt om het data ge-/verbruik en netwerkgebruik in kaart te brengen van haar abonnees met een (prepaid of postpaid) data abonnement. De persoonsgegevens zijn voor KPN direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon, omdat KPN een koppeling(smogelijkheid) heeft met de unieke klant- en/of toestel identifier(s) (bijvoorbeeld het telefoonnummer), NAW-gegevens en/of (een) e-mailadres(sen). Er kan dus een relatie tussen de (persoons)gegevens worden gelegd.

De persoonsgegevens zijn in dit rapport ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het telefoonnummer), zendmastgegevens (Cell ID), de starttijd en eindtijd van de data sessie, verbruikte datavolume, URL's etc.)
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer

KPN verwerkt(e) de persoonsgegevens voor vier doeleinden:

- netwerkplanning en -beheer;
- het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed (hierna 'prepaidverkeer' genoemd);
- het gebruik van firewalls, spamfilters en virusscanners (hierna 'spam- en virusfiltering' genoemd);
- de behandeling van klantklachten (het oplossen van technische incidenten en klantproblemen in individuele gevallen).

KPN inspecteert meestal alleen gegevens óver het dataverkeer, niet de inhoud ervan. De gegevens over het dataverkeer kunnen toch inhoudskenmerken bevatten, zoals informatie over bezochte websites en gebruikte apps.

Dat soort gegevens die iets (kunnen) zeggen over het gedrag van mensen op internet zijn gevoelige persoonsgegevens waaruit informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie volgt. Alleen gedownloade bestanden en verzonden en ontvangen e-mails inspecteert en analyseert KPN ook op inhoud om spam, virussen en malware tegen te houden en te verwijderen.

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Eén van die eisen is dat er een rechtvaardigingsgrond (grondslag) moet zijn voor de verwerking. Het CBP heeft bij KPN gedurende het onderzoek een aantal overtredingen van de Wbp en de Tw geconstateerd die inmiddels zijn beëindigd.

Netwerkplanning en -beheer

Het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde netwerkplanning en -beheer is op grond van artikel 11.5 van de Tw jo. artikel 8 van de Wbp alleen toegestaan als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze onomkeerbaar te anonimiseren.

Omdat KPN de verzamelde persoonsgegevens niet direct, onomkeerbaar anonimiseerde, terwijl dat wel mogelijk is en was, had zij geen grondslag voor de gegevensverwerking voor het doeleinde netwerkplanning en -beheer (daaronder begrepen het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie). Hierdoor handelde KPN in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Prepaidverkeer

Om prepaid abonnees in staat te stellen opwaardeersites te bezoeken als hun tegoed op is, verwerkte KPN URL's om de gratis opwaardeersites te herkennen. KPN verwerkte voor dit doeleinde persoonsgegevens van méér abonnees dan alleen degenen met een ontoereikend prepaid tegoed, terwijl er ook andere mogelijkheden zijn en waren. Omdat deze gegevensverwerking onevenredig was, handelde KPN hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

Spam- en virusfiltering en klachtbehandeling

KPN heeft wel een wettelijke grondslag voor de verwerking ten behoeve van spam- en virusfiltering en klachtbehandeling. Op deze punten is KPN dan ook niet in overtreding (geweest).

Meldingsplicht

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen op grond van artikel 27 jo. 28 van de Wbp verplicht deze gegevensverwerking te melden bij het CBP. De meldingen van KPN waren niet volledig en niet duidelijk genoeg over het verwerken van persoonsgegevens ten behoeve van prepaidverkeer en spam- en virusfiltering. KPN handelde hierdoor in strijd met artikel 27 jo. 28 van de Wbp.

Uitdrukkelijk omschreven en gerechtvaardigde doeleinden

Doordat KPN de hiervoor genoemde twee doeleinden prepaidverkeer en spam- en virusfiltering waarvoor zij persoonsgegevens verwerkt(e) onvolledig en onvoldoende duidelijk had omschreven bij de meldingen die zij bij het CBP had gedaan, werden de door KPN verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelde KPN daarmee ook in strijd met artikel 7 van de Wbp.

Doordat de gegevensverwerking voor de doeleinden netwerkplanning en -beheer en prepaidverkeer niet in alle stadia kon steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, werden de door KPN verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelde KPN daarmee ook in strijd met artikel 7 van de Wbp.

Informeren abonnees

KPN is wettelijk verplicht abonnees 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. KPN informeerde abonnees niet over de toepassing van data-analyse technieken voor de doeleinden netwerkplanning- en beheer en prepaidverkeer. Daarnaast informeerde KPN hen niet over de soorten verkeersgegevens en de bewaartermijn. KPN handelde hierdoor in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

Verdere verwerking

Het is niet behoorlijk en niet zorgvuldig dat KPN eenmalig (over de periode februari-april 2011) op abonneeniveau gegevens heeft verstrekt over het WhatsApp-gebruik aan het KPN retailbedrijf voor marktonderzoek (analyse van de eigen dienstverlening). KPN heeft hierdoor gehandeld in strijd met artikel 6 van de Wbp.

Getroffen maatregelen

Naar aanleiding van het onderzoek heeft KPN de meldingen bij het CBP en de privacyverklaringen van het bedrijf aangepast.

KPN heeft de data-analysetools voor netwerkplanning en -beheer en prepaidverkeer stopgezet met ingang van 21 september 2012 respectievelijk 3 oktober 2012.

KPN heeft de voor netwerkplanning en -beheer opgeslagen gegevens én de geanonimiseerde gegevens die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening verwijderd.

Door deze getroffen maatregelen zijn de geconstateerde overtredingen beëindigd.

KPN heeft de data-analysetool voor netwerkplanning en -beheer aan laten passen zodat gegevens zo snel mogelijk na het verzamelen worden geanonimiseerd. Naar verwachting wordt de nieuwe versie van de software op 1 juni 2013 in gebruik genomen. Op basis van het beschikbare onderzoeksmateriaal constateert het CBP, mits KPN op adequate wijze de risico's op heridentificatie minimaliseert en doelbinding zeker stelt (gelijk zij heeft toegezegd), ten aanzien van de gegevensverwerking voor netwerkplanning en -beheer in deze specifieke context via de door KPN voorgestelde anonimiseringsoplossing geen overtreding.

Bijlage I Overzicht mobiel netwerk

AFBEELDING II data-analyse apparatuur in mobiel netwerk KPN³²³

[VERTROUWELIJK]

³²³ Bijlage 2 bij reactie KPN op verzoek om inlichtingen van 1 september 2011.

**Bijlage II Standaardlijst bijgehouden apps, websites en services [VERTROUWELIJK:
apparatuur]³²⁴**

[VERTROUWELIJK]

³²⁴ Bijlage 4 bij reactie KPN op verzoek om inlichtingen OPTA van 24 mei 2011.

Bijlage III Overzicht verwerkte gegevens, per doeleinde

Bezoek en gebruik van apps en websites ([VERTROUWELIJK: apparatuur]) tot 21 september 2012

MSISDN (identificerend gegeven van de aansluiting: het telefoonnummer)
IMSI (het daaraan gekoppelde identificerende gegeven op de SIM-kaart: het unieke klantnummer)
IMEI (identificerend gegeven van het gebruikte toestel: uniek toestelnummer; geeft informatie over het besturingssysteem)
vooraf gedefinieerde app patronen en website herkenninggegevens [VERTROUWELIJK] gelinkt aan signaleringsverkeer: • het (dynamische) IP-adres waarvandaan de gegevens kwamen (identificerende gegevens van de aansluiting(en) van de abonnees) • het IP-adres van de (web)server(s) • poortnummer • gebruikt protocol • frequentie (het aantal keren dat verbinding wordt gemaakt) • referer (laatst bezochte URL)
hostname van de applicatieserver (URL op hoofddomein)
[VERTROUWELIJK]
starttijd en eindtijd sessie
verbruikte datavolume (aantallen bytes/packets)
[VERTROUWELIJK] ³²⁵

Firewalls, spamfilters en virusscanners

unieke klant- en/of toestelidentificer(s)
inhoud van door abonnees (gedownload) bestanden en verzonden en ontvangen e-mails aan de hand van vooraf gedefinieerde spam-, virus- en malware-herkenningsspatronen, voor zover nodig om spam/virussen/malware tegen te houden en te verwijderen (spam-, virus- en malware-herkenninggegevens)

Prepaidverkeer [VERTROUWELIJK: apparatuur] tot 3 oktober 2012

unieke klant- en/of toestelidentificer(s)
URL

Behandeling van klantklachten

unieke klant- en/of toestelidentificer(s)
performance informatie / status
inhoud van het dataverkeer, voor zover het voor de behandeling van de klantklacht noodzakelijk is om dit te openen

³²⁵ Zienswijze 1 KPN, p. 51-56.

Bijlage IV Verklarende woordenlijst

APN (Access Point Name)	Naam van het externe netwerk waarmee de GGSN verbinding legt, zoals het internet of bijvoorbeeld de MMS-server.
Core netwerk	Het core netwerk van een mobiele operator verzorgt het afwickelen van telefonie- en dataverkeer vanaf het netwerk van zendmasten. Het core netwerk stelt mobieltjes in staat om onderling met elkaar te communiceren en met mobieltjes van andere (wereldwijde) operators.
Fair Use Policy	Term die door operators en providers wordt gebruikt om 'normaal datagebruik' te omschrijven, in tegenstelling tot abonnementen met een vaste hoeveelheid toegestaan dataverkeer per maand.
GGSN (<i>Gateway GPRS Support Node</i>)	Netwerkapparatuur die de signaleringen en het dataverkeer doorgeeft aan externe netwerken, zoals het internet.
GPRS (<i>General Packet Radio Service</i>)	Standaard voor het afwickelen van mobiel dataverkeer.
GSM (<i>Global System for Mobile Communications</i>)	Standaard voor het afwickelen van mobiel spraakverkeer. Sinds midden jaren negentig kan via GSM ook dataverkeer worden afgewikkeld. Dat wordt ook wel 2G-verkeer genoemd, <i>Second Generation Wireless Digital Technology</i> .
Hash	Wiskundige berekening die grotere dataverzamelingen van verschillende omvang kan omzetten naar kleinere dataverzamelingen met een vaste lengte.
HLR (<i>Home Location Register</i>)	Database met eigenschappen van het mobiele abonnement: prepaid of abonnement, wel of niet mogen bellen in het buitenland (roaming), doorschakelingen, blokkades, enz. De HLR houdt ook de geografische positie van het toestel bij (via zendmastgegevens uit het VLR).
IMEI (<i>International Mobile Equipment Identity</i>)	Wereldwijd uniek 15-cijferig nummer in de hardware van smartphones, waarmee ook de fabrikant van het besturingssysteem kan worden herkend, zoals Blackberry (RIM), Android (Google) of iOS (Apple).
IMSI (<i>International Mobile Subscriber</i>)	Voor klanten van mobiele telefonie

<i>Identity)</i>	wereldwijd uniek 15-cijferig nummer, opgeslagen op de SIM-kaart van de mobiele telefoon. De eerste drie nummers zijn de landcode (in Nederland bijvoorbeeld 204), gevolgd (in Europa) door twee nummers die de aanbieder van het netwerk in dat land identificeren waar de klant abonnee is.
<i>MSISDN (Mobile Subscriber Integrated Services Digital Network-Number)</i>	Wereldwijd uniek telefoonnummer. Een MSISDN bestaat uit maximaal 15 posities, beginnend met de landcode, gevolgd door een netnummer en de tien nummers van het eigenlijke telefoonnummer (in Nederland: 06-nummer).
<i>MVNO (Mobile Virtual Network Operator)</i>	Een (MVNO) is een bedrijf dat niet over een licentie beschikt, maar onder eigen merknaam mobiele telefonie verkoopt over het netwerk van een andere mobiele operator.
Radiotoegangsnetwerk	Het radiotoegangsnetwerk van een mobiele operator verzorgt het afwikkelen van telefonie- en dataverkeer via het netwerk van zendmasten.
Radioweg	De radioweg ofwel air-interface is het deel van de communicatieketen dat toegang biedt tot het radiotoegangsnetwerk.
Roaming	Techniek om gespreks- en dataverkeer van de eigen klanten door te leiden naar andere netwerkoperators in het buitenland (en daarvoor de kosten in rekening te kunnen brengen bij de andere operator).
<i>SGSN (Serving GPRS Support Node)</i>	Netwerkapparatuur die mobiel data- en signaleringsverkeer afwikkelt van en naar zendmasten in het (eigen) netwerk. De SGSN houdt tevens locatiegegevens bij op zendmastniveau, en speelt een kernrol bij de authenticatie van abonnees en het factureren.
Signalering	Kleine berichten die nodig zijn om de verbinding op te bouwen, in stand te houden en te verbreken.
<i>UMTS (Universal Mobile Telecommunications Service)</i>	Standaard voor het afwikkelen van breedband mobiel dataverkeer, ook wel 3G genaamd. UMTS is de opvolger van GPRS als standaardtechnologie om mobiel dataverkeer af te wikkelen.
<i>VLR (Visitor Location Register)</i>	Database met de exacte locaties van alle

	abonnees in het eigen service-gebied van de operator. Deze informatie is noodzakelijk om gesprekken af te leveren bij de juiste zendmast.
--	---

Bijlage V Zienswijze 1 KPN op de Voorlopige Bevindingen, met de reactie daarop van het CBP (zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd én aangevuld in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van dat Conceptrapport definitieve bevindingen).

Opmerkingen en aanvullingen feitelijk kader

Zienswijze 1 KPN: KPN geeft in haar zienswijze een technische toelichting op haar mobiele netwerk(infrastructuur).³²⁶

In haar zienswijze voegt KPN daaraan toe dat het GSM-gedeelte en het GPRS-gedeelte in verbinding met elkaar staan, resources delen en in grote mate afhankelijk zijn van elkaar: *“Van belang hierbij is dat het mobiele KPN netwerk zowel voor belverkeer als voor dataverkeer een maximumcapaciteit heeft. (...) Als dit maximum wordt overschreden, is er een risico dat het betreffende [GPRS-, toevoeging door het CBP] netwerkonderdeel crasht. (...) Indien dit tot gevolg heeft dat ook het radiotoegangsnetwerk crasht, zal ook niet meer mogelijk zijn om te bellen via het GSM-gedeelte.”*³²⁷

KPN schrijft dat vanaf het derde kwartaal van 2010 de signaleringscapaciteit is [VERTROUWELIJK]. Het aantal RNC's is sinds 2010 uitgebreid tot [VERTROUWELIJK]. Oude verwerkingstechnologie is vervangen door nieuwe en de verwerkingscapaciteit is [VERTROUWELIJK]. In totaal is volgens cijfers van KPN [VERTROUWELIJK] geïnvesteerd.³²⁸

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van de werking en (investeringen in) de infrastructuur van het mobiele netwerk van KPN geleid tot aanvulling en verduidelijking van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport (het vergt geen aanpassing van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat een alternatief voor de door KPN ingezette data-analysetool voor netwerkplanning en -beheer dat ervoor zorgt dat verkeersgegevens zo snel mogelijk onomkeerbaar worden geanonimiseerd op dit moment proportioneel is).

OSI-model

Zienswijze 1 KPN: KPN stelt in reactie op het rapport voorlopige bevindingen dat het CBP de bevinding dat KPN zowel verkeersgegevens als inhoud van de communicatie verwerkt, baseert op een onjuiste weergave en analyse van het OSI-model. KPN merkt op dat de conclusie van het CBP dat het analyseren van de applicatielaag (OSI-laag 7) per definitie meebrengt dat de inhoud van de communicatie wordt bekeken, niet juist is. Verder is voor dataverkeer het meest toegepaste model volgens KPN het “TCP/IP”-model.³²⁹

³²⁶ Zienswijze 1 KPN, p. 28-30.

³²⁷ Idem, p. 32; zie ook idem, p. 24-31.

³²⁸ Idem, p. 37-38.

³²⁹ Idem, p. 25, 40-43; zie in dezelfde zin idem, p. 45.

Reactie CBP: Het OSI-model wordt hier niet gebruikt als een normatief model dat voorschrijft op welke wijze een telecommunicatienetwerk moet zijn ingericht, maar als hulpmiddel om processen en gegevensstromen in een netwerk te kunnen aanduiden. De omstandigheid dat zo'n model altijd een vereenvoudiging is van de werkelijkheid, doet niet af aan de waarde daarvan als hulpmiddel. Ter vergelijking is tevens de indeling van netwerkverkeer in het TCP-IP model opgenomen in dit rapport. Het kan overigens nog eenvoudiger. Het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, deelt in de recente concept netneutraliteitsrichtsnoeren het netwerkverkeer in twee lagen in, te weten: een netwerklaag en een applicatie/contentlaag. BEREC schrijft: *"When running an application, the end user is making use of the electronic communication service at the network layer. The application software installed on the terminal equipment (also referred to as the host) executes functions at the application/content layer (...). Applications (e.g. telephony, television and web) and content (e.g. videos and web pages) are produced in the endpoints which communicate with each other using the underlying network layer. In these guidelines, the content/application layer is referred to simply as the application layer, while recognising that it actually contains both content and applications."*³³⁰

Het CBP stelt niet dat het enkele feit dat KPN ook gegevens uit de applicatielaag inspecteert en analyseert, zonder meer meebrengt dat KPN tevens inhoud van de communicatie verwerkt. Ten aanzien van spamfiltering en virus- en malwarebestrijding geldt echter dat KPN, zoals zij in haar zienswijze ook aangeeft, niet alleen headergegevens, maar ook inhoud van e-mails en bestanden inspecteert en analyseert om spam, virussen en malware te herkennen.

De zienswijze 1 van KPN heeft op het punt van (het gebruik van) het OSI-model geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Statistisch betrouwbare analyses van trends in het mobiele netwerk

Zienswijze 1 KPN: KPN schrijft in haar zienswijze dat de verwerkte gegevens uitsluitend worden gebruikt voor kwantitatief statistisch en technisch onderzoek. Met dit onderzoek wordt beoogd om uitspraken te doen over netwerkbelasting en netwerkgebruik en de verwachte toename daarvan (het betreffen dus trendanalyses).³³¹ In haar zienswijze voegt KPN daaraan toe dat de data-analyse volgens KPN noodzakelijkerwijs wordt uitgevoerd op niet-geanonimiseerde data: *"Wanneer het KPN [VERTROUWELIJK] de gegevens direct bij verzameling onomkeerbaar zou anonimiseren, wordt het voor haar onmogelijk om trends op individueel gebruikers niveau te volgen. Dit zou betekenen dat KPN uitsluitend een algemene extrapolatie zou zien van de absolute stijging in bijvoorbeeld algemene signalen. Dit is onvoldoende om voorspellingen te kunnen doen voor benodigde uitbreidingen in het netwerk. Bij anonimisering kan bijvoorbeeld niet worden gezien of bepaalde gebruikers meer dan andere gebruikers bijvoorbeeld gebruik*

³³⁰ BEREC Guidelines for Quality of Service in the scope of Net Neutrality. Draft for public consultation, dated 29 May 2012, p. 15-16. URL: http://berec.europa.eu/doc/consult/bor_12_32_guidelines.pdf.

³³¹ Zienswijze 1 KPN, p. 49.

*maken van bepaalde apps, op basis waarvan voorspellingen kunnen worden gedaan. Als bijvoorbeeld in bepaalde gebieden veel jonge mensen wonen en 'early adopters' zal meer uitbreiding van het netwerk nodig zijn, dan in gebieden waar dit niet het geval is. Anonimisering betekent ook dat het onmogelijk wordt om überhaupt dergelijke gebruikersgroepen te identificeren.*³³²

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van de noodzaak van data-analyse geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

(Header)informatie in het eerste datapakket met een client request

Zienswijze 1 KPN: In haar zienswijze licht KPN haar werkwijze als volgt nader toe. Het KPN [VERTROUWELIJK] past data-analyse technologieën toe voor het maken van voorspellingen over toename in dataverkeer in het kader van haar netwerkplanning en -beheer. Daartoe moet KPN, zo betoogt zij, zowel kijken naar het signaleringsverkeer dat via het GTP-C kanaal wordt vervoerd als naar het dataverkeer dat via het GTP-U kanaal loopt: op basis van louter het signaleringsverkeer is het volgens KPN niet mogelijk om te onderscheiden op welke soort dataverkeer (bijvoorbeeld welke apps) de signaleringen betrekking hebben (dataverkeer moet worden gecorreleerd met specifieke signaleringen). [VERTROUWELIJK].³³³

KPN licht in haar zienswijze nader toe dat de data-analyse apparatuur die KPN inzet telkens uitsluitend de (header) informatie inspecteert in het eerste datapakket met een client request (van de reeks die samen een bericht vormen) dat naar de applicatieserver gaat: *“Wat er terugkomt aan informatie vanaf de server wordt niet bekeken (hierin zit de inhoud van een webpagina bijvoorbeeld).”*³³⁴ KPN merkt daarbij op: *“de data-analyse technieken die KPN toepast, inspecteren verder niet alle eerste pakketjes die over het GTP-U kanaal worden vervoerd. KPN selecteert alleen die apps die naar verwachting het meeste signaleringsverkeer veroorzaken (...) Door slechts de vooraf bepaalde applicaties te correleren met de bijbehorende signaleringen, verwerkt KPN op het GTP-C kanaal ook slechts die signaleringen die verband houden met de internetssessie van deze applicaties.”*³³⁵

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van (de werkwijze van KPN bij) de inzet van data-analyse technieken geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Het faciliteren van toegang tot (gratis) opwaardeersites en de facturering van MMS-verkeer

Zienswijze 1 KPN: KPN licht in haar zienswijze toe dat de [VERTROUWELIJK] naar de URL van de website (onderdeel van de “client request”-header in de

³³² Idem, p. 49; zie ook idem, p. 51-53.

³³³ Idem, p. 38-39 en 45.

³³⁴ Idem, p. 43-44.

³³⁵ Idem, p. 46.

applicatielaag) kijkt. Wanneer het een URL betreft van een gratis opwaardeersite, verleent de [VERTROUWELIJK] de prepaid abonnee toegang.³³⁶

KPN licht in haar zienswijze toe dat het netwerksysteem van KPN MMS standaard als 'normaal dataverkeer' beschouwt. Om dat te voorkomen [VERTROUWELIJK]. Als het een MMS is, wordt het volume van de MMS afgetrokken van het totale dataverbruik binnen de databundel.³³⁷

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van (de werkwijze van KPN bij) de inzet van data-analyse technieken geleid tot verduidelijking en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op het punt van het faciliteren van toegang tot (gratis) opwaardeersites niet geleid tot aanpassing van de conclusies in het rapport (de zienswijze 2 van KPN heeft op dit punt wel geleid tot aanpassing van de conclusies). De inzet van data-analyse technieken voor de facturering van MMS-verkeer is naar aanleiding van de zienswijze 1 van KPN buiten de scope van dit onderzoek verklaard.

Verdere verwerking

Zienswijze 1 KPN: KPN verklaart dat de [VERTROUWELIJK] die beschikking had over de gegevens, het IMSI-nummer heeft gebruikt om gebruik van WhatsApp, leeftijdsgroep etc. af te kunnen leiden, zodat gebruiksgroepen konden worden onderscheiden.³³⁸

KPN verklaart in haar zienswijze verder hierover: *"De verstrekking aan de afdeling [VERTROUWELIJK] was niet in overeenstemming met de interne [VERTROUWELIJK] procedures. [VERTROUWELIJK] Zodra het management van KPN kennis kreeg van dit incident is het incident onderzocht, is de analyse direct stopgezet en zijn nadere organisatorische maatregelen genomen om herhaling te voorkomen. De betrokken personen bij het incident zijn allen specifiek hierop aangesproken."*³³⁹

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van (de werkwijze van KPN bij) de inzet van data-analyse technieken geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Samenloop Wbp en Tw: grondslagtoetsing

Zienswijze 1 KPN: Voor verkeersgegevens zijn de grondslagen volgens KPN uitputtend gespecificeerd in de Tw. Er is, zo betoogt zij, geen ruimte om de gegevensverwerking te baseren op andere grondslagen als genoemd in de Wbp.³⁴⁰

³³⁶ Idem, p. 63.

³³⁷ Idem, p. 62.

³³⁸ Idem, p. 69.

³³⁹ Idem.

³⁴⁰ Idem, p. 23.

Reactie CBP: Het CBP heeft in dit Conceptrapport definitieve bevindingen vastgesteld dat de persoonsgegevens kunnen worden ingedeeld in twee categorieën:

1. persoonsgegevens die tevens communicatie zijn (en dus geen verkeersgegevens), namelijk gegevens zoals hostnames (URL op hoofddomein), referers (laatst bezochte URL) en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer
2. persoonsgegevens die tevens verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het telefoonnummer), zendmastgegevens (Cell ID), de starttijd en eindtijd van de data sessie, verbruikte datavolume etc.

Elke categorie van persoonsgegevens heeft een eigen beoordelingskader.

Persoonsgegevens, tevens communicatie: hostnames, referers en spam-, virus- en malwareherkenningsgegevens

Ten aanzien van hostnames, referers en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer, geldt dat geen sprake is van verkeersgegevens, maar van communicatie (tevens persoonsgegevens).³⁴¹ Artikel 8 van de Wbp is van toepassing, zij het dat (richtlijnconforme uitleg³⁴² van) artikel 5, eerste lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw (nieuw)), voor zover voor dit onderzoek van belang, op dit punt een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen.

Persoonsgegevens, tevens verkeersgegevens: overige gegevens over het dataverkeer

Ten aanzien van de overige gegevens over het dataverkeer, geldt dat sprake is van persoonsgegevens, tevens verkeersgegevens. Artikel 8 van de Wbp is van toepassing, zij het dat artikel 11.5 van de Tw op dit punt een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp.

De zienswijze 1 van KPN heeft op het punt van de samenloop van Wbp en Tw, meer in het bijzonder de toetsing van de grondslag voor (i) de verwerking van persoonsgegevens die ook verkeersgegevens zijn en (ii) de verwerking van communicatie, tevens persoonsgegevens, geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat de door KPN ingezette data-analysetools voor netwerkplanning en -beheer en het faciliteren van toegang tot (gratis) opwaardeersites niet proportioneel zijn.

Verwerking van persoonsgegevens

Zienswijze 1 KPN: In haar zienswijze brengt KPN naar voren dat nu door KPN een strikte scheiding is aangebracht tussen het KPN [VERTROUWELIJK], en de door KPN

³⁴¹ Subsidiair is sprake van zowel verkeersgegevens als communicatie. Meer subsidiair valt hieruit in elk geval informatie over de communicatie af te lezen zodat deze gegevens dezelfde bescherming als de communicatie-inhoud zouden moeten genieten.

³⁴² Een bepaling van een richtlijn die niet (volledig) tijdig en correct is omgezet, dient richtlijnconform te worden geïnterpreteerd. Zie o.a. HvJ EG 5 oktober 2004, gevoegde zaken C- 397/01 tot C-403/01 (*Pfeiffer*).

verwerkte verkeersgegevens niet voor marketingdoeleinden kunnen en worden gebruikt, deze verkeersgegevens geen persoonsgegevens betreffen.³⁴³ [VERTROUWELIJK].³⁴⁴

Reactie CBP: Het is niet het criterium of KPN de bedoeling heeft om de gegevens over en uit het dataverkeer of voor dat doeleinde of andere doeleinden te gebruiken, maar of de gegevens daarvoor kunnen worden gebruikt. In de wetsgeschiedenis bij de Wbp is in dat verband opgemerkt: *“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.”*³⁴⁵ Het gebruik voor een op de persoon gericht doel is mogelijk. [VERTROUWELIJK].³⁴⁶

De zienswijze 1 van KPN heeft op het punt van [VERTROUWELIJK] geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat KPN persoonsgegevens verwerkt.

Zienswijze 1 KPN: In haar zienswijze geeft KPN aan dat ten aanzien van prepaid abonnees geldt dat verstrekking van NAW-gegevens niet verplicht is en dat zij niet over NAW-gegevens van al haar prepaid abonnees beschikt, zodat de verkeersgegevens niet als persoonsgegevens kunnen worden aangemerkt.³⁴⁷

Reactie CBP: Ten aanzien van de prepaid abonnees van wie KPN geen NAW-gegevens en/of e-mailadressen heeft, beschikt KPN wel over ten minste het MSISDN (een direct contactgegeven), IMSI- en IMEI-nummer, IP-adres³⁴⁸ en locatiegegevens met tijd.

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29-werkgroep over het begrip persoonsgegeven is hierover opgemerkt: *“(…) 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. (…) Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar*

³⁴³ Zienswijze 1 KPN, p. 12.

³⁴⁴ Idem, p. 68 en bijlage VIII bij deze zienswijze.

³⁴⁵ Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

³⁴⁶ KPN heeft dit in haar zienswijze erkend. Zienswijze 1 KPN, p. 69.

³⁴⁷ Idem, p. 13.

³⁴⁸ Zie HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), r.o. 26 over de status van IP-adressen, die persoonsgegevens vormen.

naam te achterhalen. De definitie van “persoonsgegevens” weerspiegelt ook dit feit”, (onderstreping toegevoegd door het CBP).³⁴⁹

Wanneer gegevens gekoppeld worden aan een uniek nummer is doorgaans sprake van een geïndividualiseerd persoon. Het CBP verwijst in dat verband ook naar de overweging in het arrest van het Hof van Justitie van de EG van 6 november 2003 dat “(...) *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, als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens in de zin van artikel 3, lid 1, van richtlijn 95/46 is aan te merken.*”³⁵⁰

Reactie CBP: De zienswijze 1 van KPN heeft op het punt van de identificeerbaarheid van de prepaid abonnees geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Zienswijze 1 KPN: Onder verwijzing naar het voorbeeld in de wetsgeschiedenis bij de Wbp over de netwerkbeheerder die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, brengt KPN in haar zienswijze naar voren dat nu door KPN een strikte scheiding is aangebracht tussen het KPN [VERTROUWELIJK], en de door KPN verwerkte verkeersgegevens niet voor marketingdoeleinden kunnen en worden gebruikt, deze verkeersgegevens geen persoonsgegevens betreffen.³⁵¹

Reactie CBP: Indien KPN met deze stelling bedoelt te zeggen dat om die reden geen sprake is van verwerking van persoonsgegevens, geldt dat het enkele feit dat KPN in haar mobiele netwerk data-analyse technieken kan toepassen en toepast maakt dat geen sprake is van *mere conduit* (louter doorvoer).

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Onderscheid verkeersgegevens en communicatie

Zienswijze 1 KPN: geeft aan dat de gegevens die KPN verwerkt door middel van toepassing van data-analyse technieken uitsluitend verkeersgegevens betreffen en niet de inhoud van communicatie (met uitzondering van geautomatiseerde scans door firewalls, virusscanners en spamfilters).³⁵²

KPN stelt dat een URL een verkeersgegeven betreft, omdat een URL wordt omgezet in een IP-adres.³⁵³

³⁴⁹ WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 14-15.

³⁵⁰ HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

³⁵¹ Zienswijze 1 KPN, p. 11-12.

³⁵² Idem, p. 25.

³⁵³ Idem, p. 10.

Reactie CBP: Het CBP heeft in het Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat een URL communicatie is. Er kan onderscheid worden gemaakt tussen de inhoudelijke vraag (Get request URL) en de nummerreeks van de webserver (IP-adres).

De zienswijze 1 van KPN heeft op het punt van het onderscheid tussen verkeersgegevens en communicatie geleid tot verduidelijking en aanvulling van het toepasselijke en toegepaste wettelijk kader. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat een URL communicatie is (de zienswijze 2 van KPN heeft op dit punt wel geleid tot aanpassing van de conclusies).

Zienswijze 1 KPN: KPN betwist dat verkeersgegevens gevoelige gegevens zijn. De vraag of de verwerking van deze verkeersgegevens gevoelig is (mogelijk een impact heeft op de privacy van betrokkenen of niet) hangt volgens KPN af van het doel waarvoor deze gegevens vervolgens worden gebruikt. Als verkeersgegevens worden verwerkt voor de toegestane doeleinden op grond van de Tw (waaronder overbrenging van communicatie) is de impact op de privacy van gebruikers minimaal en betreffen dit volgens KPN geen gevoelige gegevens. Bovendien is het onderscheid gevoelige / niet-gevoelige persoonsgegevens hier volgens KPN niet relevant, nu de wetgever in de Tw het onderscheid naar aard van gegevens reeds tot uitdrukking heeft laten komen in het onderscheid tussen verkeersgegevens en communicatie.³⁵⁴

Reactie CBP: Het CBP heeft in het Conceptrapport definitieve bevindingen onder verwijzing naar de (antwoorden op de vragen over) het kabinetsstandpunt over het rapport van de Commissie Grondrechten in het digitale tijdperk gemotiveerd vastgesteld dat verkeersgegevens gevoelige gegevens zijn. KPN gaat eraan voorbij dat persoonsgegevens, tevens verkeersgegevens zoals de gegevens over locatie en het bezoek aan en gebruik van apps en websites wel degelijk mogelijk een impact kunnen hebben op de privacy van betrokkenen. Het enkele feit dat de wetgever (ook) een onderscheid maakt tussen verkeersgegevens en communicatie maakt dat niet anders.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport dat verkeersgegevens gevoelige gegevens zijn.

Mogelijke grondslagen voor de inzet van data-analyse tools

Netwerkplanning en -beheer

Zienswijze 1 KPN: In haar zienswijze stelt KPN zich op het standpunt dat voor zover er sprake is van de verwerking van persoonsgegevens verschillende van de in artikel 8 van de Wbp opgesomde grondslagen daaraan ten grondslag kunnen worden gelegd, te weten: uitvoering van de overeenkomst met de betrokken abonnees (artikel 8, aanhef en onder b, van de Wbp) en ter naleving van wettelijke verplichtingen (artikel 8, aanhef en onder c, van de Wbp).³⁵⁵

³⁵⁴ Idem, p. 13-14.

³⁵⁵ Idem, p. 23.

KPN stelt zich in haar zienswijze primair op het standpunt dat nu KPN geen behoorlijk netwerkmanagement kan voeren indien zij de gegevens geanonimiseerd dient te verwerken, niet relevant is dat er data-analyse technieken op de markt zijn die mogelijk gegevens kunnen anonimiseren direct na opslag.³⁵⁶ KPN stelt verder in reactie op het rapport voorlopige bevindingen niet bekend te zijn met andere technische oplossingen die dit zouden kunnen of die deze doeleinden ook op een andere, minder ingrijpende manier, zouden kunnen bereiken, en verklaart: *“Nogmaals, het is niet aan KPN om dit te bewijzen, maar aan het CBP om het noodzakelijke feitenonderzoek te doen om haar Voorlopige bevindingen te staven.”*³⁵⁷

Reactie CBP: Het is niet aan het CBP om zich op detailniveau in te laten met de door KPN te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch alternatief voor te schrijven). Het is aan KPN om onrechtmatige toepassingen van de data-analyse techniek te voorkomen. In dat verband spelen het proportionaliteits- en subsidiariteitsvereiste een rol (oftewel, is de inbreuk op de belangen van de bij de verwerking betrokkenen evenredig in verhouding tot het met de verwerking te dienen doel en kan het doeleinde niet anderszins of met minder ingrijpende middelen worden bereikt). De aangehaalde voorbeelden van technische alternatieven in dit Conceptrapport definitieve bevindingen worden gebruikt om aan te tonen dat er andere mogelijkheden, en minder ingrijpende middelen zijn, om hetzelfde resultaat te bereiken. Hieruit volgt dat de huidige wijze van verwerken van persoonsgegevens op individueel persoonsniveau, althans geaggregeerd per abonnee niet ‘noodzakelijk’ en ‘in overeenstemming met het subsidiariteitsbeginsel’ is. Het CBP heeft hiervoor in dit Conceptrapport definitieve bevindingen tevens gemotiveerd vastgesteld dat om trends in gebruikersverkeer te identificeren, voor netwerkplanning (forecasting), de persoonsgegevens kunnen worden geaggregeerd naar gebruikersgroepniveau of netwerkelement en onomkeerbaar kunnen worden ontdaan van persoonsidentificerende kenmerken.³⁵⁸ Hieruit volgt dat de huidige wijze van verwerken van persoonsgegevens op individueel persoonsniveau, althans geaggregeerd per abonnee ook niet ‘noodzakelijk’ en ‘proportioneel’ is.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport dat een alternatief voor de door KPN ingezette data-analysetools dat ervoor zorgt dat verkeersgegevens direct onomkeerbaar worden geanonimiseerd op dit moment proportioneel is.

Zienswijze 1 KPN: KPN verklaart dat zij op grond van de (gewijzigde) Tw een aantal wettelijke plichten heeft.³⁵⁹

Reactie CBP: KPN betoogt, zo begrijpt het CBP, dat nodig is dat gebruik wordt

³⁵⁶ Idem, p. 56; zie ook idem, p. 61.

³⁵⁷ Idem, p. 59; zie ook idem, p. 61.

³⁵⁸ KPN zou bijvoorbeeld een tussenstap kunnen inbouwen in het anonimiseringsproces, met tijdelijke pseudoniemen. Zie CBP Rapport van bevindingen over de verwerking van geolocatiegegevens door TomTom N.V. van 20 december 2011. URL: http://www.cbpreweb.nl/downloads_pb/pb_20120112_tomtom-geolocatie-persoonsgegevens-definitieve-bevindingen.pdf.

³⁵⁹ Zienswijze KPN van 24 februari 2012, p. 17-20.

gemaakt van netwerkmanagement-toepassingen, waarmee de verschillende verkeersstromen op het netwerk op het niveau van de individuele abonnees in kaart worden gebracht, om aan verschillende wettelijke verplichtingen te kunnen voldoen, waaronder artikel 20 van de Universeledienstrichtlijn.³⁶⁰

Artikel 20 van de Universeledienstrichtlijn (geïmplementeerd in artikel 7.1, eerste en vijfde, lid, van de Tw jo. artikel 3.5b van het Besluit universele dienstverlening en eindgebruikersbelangen (nieuw); hierna: BUDE) stelt regels over het specificeren in het contract met de abonnee van onder andere (i) informatie over eventuele beperkingen inzake toegang tot en/of gebruik van diensten en toepassingen, voor zover rechtens toegestaan (ii) de minimumkwaliteitsniveaus van de geboden diensten en (iii) door de onderneming ingestelde procedures om het verkeer te meten en te sturen, om te voorkomen dat een netwerkaansluiting tot haar maximum wordt gevuld of overloopt, en over de wijze waarop deze procedures gevolgen kunnen hebben voor de kwaliteit van de dienstverlening. Dit artikel regelt transparantieplichtingen. Uit dit artikel vloeit naar zijn aard geen wettelijke verplichting voort om met toepassing van data-analyse technieken deze gegevens te verwerken. Er bestaat geen evident verband tussen de verwerking van de (gevoelige) persoonsgegevens op persoonsniveau, zoals die thans door KPN plaatsvindt, en de transparantieplichtingen.

Indien en voor zover KPN zich ten aanzien van dit doeleinde netwerkplanning en -beheer beroept/wenst te beroepen op de grondslag wettelijke plicht (artikel 8, aanhef en onder c, van de Wbp), een verplichting die zou voortvloeien uit een of meerdere van de hieronder genoemde wetsartikelen³⁶¹, stelt het CBP het volgende vast.

Ad artikel 11.2 van de Tw (zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer)

Artikel 11.2 van de Tw expliciteert dat aanbieders zorg moeten dragen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers (bijvoorbeeld door het aantal persoonsgegevens tot het strikt noodzakelijke minimum te beperken).

Uit dit artikel vloeit naar zijn aard geen wettelijke verplichting voort om met toepassing van data-analyse technieken deze gegevens te verwerken. Er bestaat geen evident verband tussen de verwerking van de (gevoelige) persoonsgegevens op persoonsniveau, zoals die thans door KPN plaatsvindt, en de (uitvoering van de) algemene zorgplicht. De gegevensverwerking is geen noodzakelijk uitvloeisel van de algemene zorgplicht, maar heeft tot doel trends in gebruikersverkeer te kunnen identificeren voor netwerkplanning (forecasting).

Ad artikel 11.3 van de Tw (passende technische en organisatorische maatregelen)

Artikel 11.3 van de Tw is onvoldoende specifiek om ter zake van dit doeleinde

³⁶⁰ Idem, p. 20.

³⁶¹ Het CBP heeft de toepassing van de hieronder genoemde wetsartikelen voorgelegd aan ACM en Agentschap Telecom in het kader van het Samenwerkingsprotocol CBP-OPTA onderscheidenlijk de Samenwerkingsovereenkomst Agentschap Telecom – College bescherming persoonsgegevens van beide toezichthouders. ACM en Agentschap Telecom stemmen elk voor zover zij ter zake de bevoegde toezichthouder zijn in met de voorgelegde toepassing van deze wetsartikelen.

netwerkplanning en -beheer een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en (de uitvoering van) de wettelijke verplichting.

Ad artikel 6.5 van de Tw (aankiesbaarheid niet-geografische nummers), artikel 7.7 van de Tw (toegang alarmnummers) en artikel 14.6 van de Tw (voorbereiding buitengewone omstandigheden)

Artikel 6.5 van de Tw over de aankiesbaarheid in het kader van bijvoorbeeld grensoverschrijdende abonnee-informatiediensten en -inlichtingendiensten, artikel 7.7 van de Tw over de toegang tot alarmnummers en artikel 14.6 van de Tw over de voorbereiding van buitengewone omstandigheden, zijn onvoldoende specifiek om ter zake van dit doeleinde een verplichting aan te nemen om met toepassing van data-analyse technieken (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en (de uitvoering van) de wettelijke verplichting

Ad artikel 22, derde lid, van de gewijzigde Universeledienstrichtlijn (geïmplementeerd in artikel 7.4a, vijfde lid, van de Tw (nieuw): kwaliteit van de dienst), artikel 7.4a, eerste lid, van de Tw (nieuw) (netneutraliteit) en artikel 23 van de gewijzigde Universeledienstrichtlijn (zoals geïmplementeerd in artikel 11a.1 van de Tw (nieuw): beschikbaarheid van diensten) en artikel 11a.2 van de Tw (nieuw)

Artikel 7.4a van de Tw is in werking getreden op 1 januari 2013, na verzending van het Conceptrapport definitieve bevindingen.

Artikel 7.4a, vijfde lid, van de Tw (nieuw) vormt een implementatie van artikel 22, derde lid, van de gewijzigde Universeledienstrichtlijn. Voor zover deze bepaling de *mogelijkheid* biedt minimumkwaliteitseisen te stellen aan de dienstverlening zodat een achteruitgang van de dienstverlening of een belemmering of vertraging van het verkeer via internet kan worden voorkomen, geldt dat daarmee op zichzelf geen sprake is van een wettelijke verplichting. Zulke minimumkwaliteitseisen zijn (nog) niet gesteld (bij of krachtens algemene maatregel van bestuur). Er is dus geen verplichting, opgenomen in een wettelijke bepaling, die op KPN rust en waarvan de verwerking met toepassing van data-analyse technieken van (gevoelige) persoonsgegevens op persoonsniveau een noodzakelijk uitvloeisel is.

Artikel 7.4a, eerste lid, van de Tw (nieuw), regelt de verplichting voor aanbieders om netneutraal te handelen, met daarop een aantal uitzonderingen (bijvoorbeeld om de gevolgen van congestie te beperken, waarbij gelijke soorten verkeer gelijk worden behandeld, of ter uitvoering van een wettelijk voorschrift of rechterlijk bevel). Indien en voor zover een van de uitzonderingssituaties van toepassing is, betekent dit dat de netneutraliteitsverplichting niet geldt.

Artikel 7.4a van de Tw (nieuw) was nog niet in werking getreden ten tijde van het rapport voorlopige bevindingen. Daar komt bij dat de uitzonderingen op de netneutraliteitsverplichting als geformuleerd in dit artikel 7.4a, eerste lid, van de Tw (nieuw) geen wettelijke verplichting vormen om, ter invulling van zo'n uitzonderingssituatie, met toepassing van data-analyse technieken (gevoelige) persoonsgegevens op persoonsniveau te verwerken. De uitzonderingen bepalen alleen

OPENBARE VERSIE Rapport definitieve bevindingen van 29 mei 2013 118

iets over de toelaatbaarheid van niet-netneutraal handelen. In dit verband wijst het CBP erop dat in artikel 7.4a, eerste lid, onder d, van de Tw een afzonderlijke uitzondering is geregeld op de netneutraliteitsverplichting *“ter uitvoering van een wettelijk voorschrift (...)”*: de wetgever heeft dus bedoeld dat de wettelijke verplichting moet voortvloeien uit een andere wettelijke bepaling dan het netneutraliteitsartikel. Er is dus geen verplichting, opgenomen in een wettelijke bepaling, waarvan de gegevensverwerking een noodzakelijk uitvloeisel is.

Datzelfde geldt ten aanzien van artikel 11a.1 en 11a.2 van de Tw (nieuw) over de veiligheid en integriteit van netwerken en diensten en de meldplicht voor veiligheidsinbreuken en het verlies van integriteit. Artikel 11a.1 van de Tw, over passende technische en organisatorische maatregelen om de risico's voor de veiligheid en de integriteit van netwerken en diensten te beheersen, is voor het overige ook onvoldoende specifiek om voor dit doeleinde ter zake een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Zienswijze 1 KPN: KPN betwist, zoals vermeld, dat er bij de huidige stand van zaken 'andere manieren' zijn om de integriteit en -veiligheid van haar mobiele netwerk en diensten op een verantwoorde wijze te waarborgen.³⁶²

Reactie CBP: Het is, zoals vermeld in dit Conceptrapport definitieve bevindingen, niet aan het CBP om zich op detailniveau in te laten met de door KPN te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch alternatief voor te schrijven). Het is aan KPN om onrechtmatige toepassingen van de data-analyse techniek te voorkomen. Op KPN rust de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer van de betrokkenen te vermijden dan wel zo beperkt mogelijk te houden. Gegevensverwerking is blijkens artikel 8, aanhef en onder f, van de Wbp alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook 'noodzakelijk' is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke.³⁶³ KPN heeft niet aannemelijk gemaakt dat het gebruiken, vastleggen en bewaren van de persoonsgegevens noodzakelijk is op individueel persoonsniveau, althans geaggregeerd per abonnee en dat netwerkplanning in redelijkheid *niet* op een andere, voor de betrokkenen minder nadelige wijze kan worden verwezenlijkt. KPN heeft verklaard: *“Omdat [VERTROUWELIJK] en de bevindingen in de pilot aan de verwachtingen hebben beantwoord heeft KPN geen verder onderzoek naar technische alternatieven met vergelijkbare functionaliteiten gedaan.”*³⁶⁴ KPN heeft de door het CBP aangedragen technische alternatieven onvoldoende specifiek weersproken. Het enkele feit dat KPN niet bekend

³⁶² Zienswijze 1 KPN, p. 4 en 56-61.

³⁶³ *Kamerstukken II 1998/99, 25 892, nr. 13, p. 6: “Overigens wijzen wij erop dat alleen een gerechtvaardigd belang niet voldoende is. Gegevensverwerking is blijkens artikel 8, onder f, alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook «noodzakelijk» is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke.”*

³⁶⁴ Reactie KPN op verzoek om inlichtingen van 17 oktober 2011, p. 4-5.

is met andere technische oplossingen (die direct toepasbaar zijn) binnen haar mobiele netwerk maakt niet dat de verwerking van persoonsgegevens zoals die thans door KPN plaatsvindt proportioneel en subsidiair is.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Zienswijze 1 KPN: In haar zienswijze stelt KPN zich op het standpunt dat de doeleinden waarvoor KPN de verkeersgegevens verwerkt, vallen binnen de wettelijke grondslagen in de Tw voor de verwerking van verkeersgegevens en ook overigens voldoen aan het proportionaliteitsvereiste dat in deze grondslagen is vervat.³⁶⁵ KPN verklaart dat zij de verwerking baseert op de grondslag overbrenging van communicatie, meer in het bijzonder het afgeleide doeleinde van verkeersbeheer. Deze grondslag correspondeert volgens KPN met de grondslag uitvoering van een overeenkomst (artikel 8, aanhef en onder b, van de Wbp).³⁶⁶

Reactie CBP: De verwerking van niet-geanonimiseerde verkeersgegevens is toelaatbaar indien deze noodzakelijk is voor 'verkeersbeheer'. Het CBP beoordeelt deze noodzaak als volgt.

Het CBP heeft in dit Conceptrapport definitieve bevindingenvastgesteld dat het verzamelen, gebruiken, vastleggen en bewaren van de persoonsgegevens door KPN over het bezoek aan en gebruik van apps en websites op individueel persoonsniveau, althans geaggregeerd per abonnee om inzicht te hebben/krijgen in de ontwikkelingen van verkeer, netwerkgebruik etc. in verband met de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps en websites, zoals dat thans door KPN plaatsvindt, niet 'noodzakelijk' en 'proportioneel'/'in overeenstemming met het subsidiariteitsbeginsel' is.

Nu het verzamelen, gebruiken, vastleggen en bewaren van de verwerkte persoonsgegevens door KPN over het bezoek aan en gebruik van apps en websites op individueel persoonsniveau, althans geaggregeerd per abonnee niet noodzakelijk is voor verkeersbeheer³⁶⁷, en KPN ook geen andere grondslag heeft voor deze besproken

³⁶⁵ Zienswijze 1 KPN, p. 4; zie ook idem, p. 15-22 en 60.

³⁶⁶ Idem.

³⁶⁷ Vgl. ook overweging 29 van de e-Privacyrichtlijn: "De dienstenaanbieder mag zo nodig in individuele gevallen verkeersgegevens met betrekking tot abonnees en gebruikers verwerken om technische defecten of fouten in de transmissie van communicatie op te sporen. Verkeersgegevens die nodig zijn voor facturatie mogen ook door de aanbieder worden verwerkt om op het spoor te komen van en een einde te maken aan fraude in de vorm van het niet betalen voor het gebruik van de elektronische-communicatiedienst." Hieruit kan a contrario worden afgeleid dat voor het meer algemene doel van verkeersbeheer de verwerking slechts in geaggregeerde vorm is toegelaten. Het begrip 'geaggregeerde verkeersgegevens' omvat ingevolge overweging 30 van de e-Privacyrichtlijn "verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht." De verwerking zoals die thans door KPN plaatsvindt, kan niet worden aangemerkt als verwerking in geaggregeerde vorm. Het gaat om persoonsgegevens, tevens verkeersgegevens op individueel persoonsniveau, althans op persoonsniveau geaggregeerde gegevens: (technische) persoonsgegevens over het functioneren van het netwerk bij het gebruik daarvan door een individuele betrokkene, met locatiegegevens. De verwerking van persoonsgegevens gaat verder dan de

verwerking van persoonsgegevens, handelt KPN in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp).

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Zienswijze 1 KPN: KPN stelt in haar zienswijze dat het rapport voorlopige bevindingen ten aanzien van de bevindingen in deze paragraaf onzorgvuldig is voorbereid en ontoereikend is gemotiveerd, onder andere omdat de bevindingen onder meer een impact hebben op de continuïteit en het functioneren van het mobiele KPN netwerk en KPN's mogelijkheden om te voldoen aan de kwaliteitsverplichtingen op grond van de telecommunicatiewetgeving. KPN merkt op: *"Het CBP miskent dat de keuze voor een data-analyse tool door een aanbieder van een veelheid van factoren afhangt, waaronder de geboden functionaliteiten, de beoogde toepassing en kosten."*³⁶⁸

Reactie CBP: Zoals vermeld in dit Conceptrapport definitieve bevindingen, is er geen wettelijke plicht tot de verwerking zoals die thans door KPN plaatsvindt. Het CBP neemt in aanmerking dat de bevindingen een impact kunnen hebben op het functioneren van het mobiele KPN netwerk, in die zin dat aanpassingen verricht zullen moeten worden. Dit kan kosten met zich brengen. Het CBP miskent ook niet dat de keuze voor een bepaalde soort data-analyse apparatuur van een veelheid van factoren afhangt. Dit alles maakt evenwel niet dat de verwerking zoals die thans door KPN plaatsvindt proportioneel en subsidiair is.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Prepaidverkeer

Zienswijze 1 KPN: KPN verklaart dat zij de verwerking baseert op de grondslag facturering (onder facturering dient ook het registreren van het tegoed van prepaid abonnees te worden begrepen). Deze grondslag correspondeert volgens KPN met de grondslag uitvoering van een overeenkomst (artikel 8, aanhef en onder b, van de Wbp).³⁶⁹

Reactie CBP: De verwerking van persoonsgegevens is toelaatbaar indien deze 'noodzakelijk' is voor de uitvoering van een overeenkomst (proportionaliteits- en subsidiariteitstoets). Het CBP beoordeelt deze noodzaak als volgt. Uit overweging 13 van de e-Privacyrichtlijn kan worden afgeleid dat de contractuele relatie tussen een prepaid abonnee en een verantwoordelijke een keten van een reeks opeenvolgende contracten inhoudt.

Naar analogie van de regeling van artikel 11.5, tweede lid, van de Tw, wordt onder de verwerking ten behoeve van de facturering niet alleen het opstellen van een factuur

overbrenging van communicatie en de facturering ervan. De verwerking kan dan ook niet worden gebaseerd op de grondslag facturering, meer in het bijzonder het afgeleide doeleinde verkeersbeheer (artikel 11.5, tweede jo. vijfde lid, van de Tw jo. artikel 8 van de Wbp).

³⁶⁸ Zienswijze 1 KPN, p. 57.

³⁶⁹ Idem, p. 64.

begrepen, maar ook bijvoorbeeld het registreren van het beltegoed van prepaid abonnees (en betaling van verleende toegang).³⁷⁰ De verwerking van de URL voor het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed vindt echter plaats als het beltegoed op is: bij een 'gratis' URL vraagt de data-analyse apparatuur niet (eerst) aan het factureringssysteem of de abonnee nog voldoende tegoed heeft, zodat de prepaid abonnee zonder tegoed een betalingswebsite kan bezoeken komen. Hieruit volgt dat de verwerkte gegevens niet noodzakelijk zijn voor de uitvoering van een overeenkomst (artikel 8, aanhef en onder b, van de Wbp).

Voor zover KPN voor dit doeleinde ook gegevens verwerkt van abonnees met een *postpaid* data abonnement en prepaid abonnees *met een toereikend tegoed*, omdat de data-analyse technieken niet alleen zouden kunnen worden toegepast als een prepaid abonnee geen tegoed meer heeft, geldt dat de inbreuk op de belangen van deze betrokkenen onevenredig is in verhouding tot het met de verwerking te dienen doel.

Daar komt bij dat er meerdere mogelijkheden, en minder ingrijpende middelen, zijn om hetzelfde resultaat te bereiken, te weten: het er voor zorgen dat prepaid abonnees zonder tegoed toegang hebben tot (gratis) opwaardeersites om opwaarderen te faciliteren. Bijvoorbeeld, door een technisch alternatief te gebruiken, zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een betalingswebsite kan bezoeken.

Uit het voorgaande blijkt dat de verwerking van persoonsgegevens niet kan worden aangemerkt als handelingen die *noodzakelijk* zijn voor een gerechtvaardigd belang van KPN. Om die reden kan de verwerking niet worden gebaseerd op de grondslag noodzaak (artikel 8, aanhef en onder f, van de Wbp).

Naar analogie van de regeling van artikel 11.5, derde lid, aanhef en onder a, van de Tw, geldt dat het faciliteren van toegang tot (gratis) opwaardeersites voor prepaid abonnees zonder tegoed naar zijn aard ook een verkoopactiviteit beoogt/is waarvoor toestemming is vereist.³⁷¹ Nu van ondubbelzinnige toestemming niet is gebleken en KPN ook geen andere grondslag heeft voor de in deze paragraaf besproken verwerking van persoonsgegevens, handelt KPN in strijd met artikel 8 van de Wbp.

De zienswijze 1 van KPN heeft op het punt van het faciliteren van toegang tot (gratis) opwaardeersites niet geleid tot aanpassing van de conclusies in het rapport dat een alternatief voor de door KPN ingezette data-analysetools zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een betalingswebsite kan bezoeken op dit moment proportioneel is (de zienswijze 2 van KPN heeft op dit punt wel geleid tot aanpassing van de conclusies).

Zienswijze 1 KPN: KPN brengt in haar zienswijze naar voren dat wanneer KPN prepaid abonnees doorleidt naar slechts één opwaardeerwebsite, de abonnees geen

³⁷⁰ Vgl. *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 155. Idem, nr. 13, p. 20. Deze grondslag correspondeert met de grondslag uitvoering van een overeenkomst (artikel 8, aanhef en onder b, van de Wbp).

³⁷¹ Deze grondslag correspondeert met de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp).

keuze meer hebben (de toegang tot de andere opwaardeerwebsites wordt dan geblokkeerd).³⁷² KPN stelt verder niet bekend te zijn met geschikte technische alternatieven om facturering van prepaidverkeer te realiseren zonder toepassing van data-analyse technieken.³⁷³

Reactie CBP: Het CBP heeft hierboven gemotiveerd vastgesteld dat er technische alternatieven zijn, zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een betalingswebsite kan bezoeken.

De zienswijze 1 van KPN heeft op het punt van het faciliteren van toegang tot (gratis) opwaardeersites niet geleid tot aanpassing van de conclusies in het rapport.

Firewalls, spamfilters en virusscanners

Zienswijze 1 KPN: In haar zienswijze geeft KPN aan dat “(anders dan het CBP aanneemt) het gebruik van firewalls, spamfilters en virusscanners geen zelfstandige doeleinden zijn maar middelen ter bevordering van het doel van netwerkindegriteit en -continuïteit.” Voor zover gegevensverwerking is toegestaan voor netwerkmanagement omvat dit volgens KPN de verwerking van gegevens door toepassing van deze middelen.³⁷⁴

KPN verklaart dat zij de verwerking baseert op artikel 11.3 van de Tw. Deze grondslag correspondeert volgens KPN met de grondslagen wettelijke plicht en uitvoering van een overeenkomst (artikel 8, aanhef en onder b en c, van de Wbp).³⁷⁵ KPN verwijst daarbij ook naar de opinie van de EDPS over netneutraliteit, netwerkbeheer en bescherming van persoonsgegevens.³⁷⁶

Reactie CBP: Ten aanzien van de spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer geldt dat artikel 8 van de Wbp van toepassing is, zij het dat (richtlijnconforme uitleg van) artikel 5, eerste lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw (nieuw)) een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen. Op grond van artikel 5, eerste lid, van de e-Privacyrichtlijn is het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst verboden indien de betrokken abonnees daarin niet hebben toegestemd, tenzij het bij wet is toegestaan.

Het CBP merkt op dat voor zover artikel 11.3 van de Tw verplicht tot het gebruik van firewalls, spamfilters en virusscanners, geldt dat de grondslag voor de verwerking van persoonsgegevens, tevens communicatie moet worden gevonden in artikel 8 van de Wbp.

³⁷² Zienswijze 1 KPN, p. 63.

³⁷³ Idem, p. 64.

³⁷⁴ Idem, p. 65.

³⁷⁵ Idem.

³⁷⁶ Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, dated 7 October 2011, p. 3-4. URL: [http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_\(1\)_15_rt_2011.pdf](http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf).

De zienswijze 1 van KPN heeft op het punt van firewalls, spamfilters en virusscanners niet geleid tot aanpassing van de conclusies in het rapport dat het CBP op basis van het beschikbare onderzoeksmateriaal geen overtreding heeft geconstateerd van artikel 8 van de Wbp.

Verdere verwerking en onzorgvuldigheid

Zienswijze 1 KPN: KPN betwist in haar zienswijze dat de verwerkte gegevens zijn gebruikt voor marketingdoeleinden. Dit omdat ten tijde van de pilot vanuit de [VERTROUWELIJK: apparatuur] een set met data [VERTROUWELIJK] en op geen enkel moment gekoppeld is geweest aan andere ICT-systemen binnen KPN.³⁷⁷

KPN voegt daaraan toe dat anders dan het CBP stelt de verwerking van verkeersgegevens niet is gedaan ten behoeve van marketingdoeleinden, maar ten behoeve van analyse van de dienstverlening van KPN. Direct marketing activiteiten vallen onder de afdeling [VERTROUWELIJK] van het KPN retailbedrijf, niet onder [VERTROUWELIJK]. De afdeling [VERTROUWELIJK] heeft op geen enkel moment data of informatie gekregen in het kader van de pilot.³⁷⁸ Onder marketingdoeleinden wordt volgens KPN verstaan het nauwkeurig in kaart brengen van wie (potentiële) klanten zijn om op deze personen verkoop en/of reclamestrategie af te stemmen, waardoor het mogelijk wordt bepaalde groepen van klanten - of zelfs individuele klanten - persoonlijk te benaderen met aanbiedingen die op hun gedrag, voorkeur en/of levenssituatie zijn afgestemd. Onder analyse van de dienstverlening valt volgens KPN het evalueren van de diensten op grond van het gebruik dat klanten maken (ontwikkelingen in gebruik van haar diensten, bijvoorbeeld dat bepaalde apps veel worden gebruikt), om in staat te zijn daar in haar tarifiering rekening mee te houden.³⁷⁹

KPN benadrukt dat KPN daarom niet in strijd handelt met haar eigen privacy policies, waarin is aangegeven dat KPN uitsluitend verkeersgegevens voor direct marketing zal gebruiken voor zover abonnees daarvoor toestemming hebben gegeven (een mogelijkheid waarvan zij in de praktijk overigens geen gebruik maakt).³⁸⁰

Ten slotte stelt KPN dat nu zij rechtmatig over de 'achterliggende' gegevens beschikte het daarmee ook mogelijk is dat deze gegevens worden geanonimiseerd en verder verwerkt voor analysedoeleinden ten behoeve van de dienstverlening.³⁸¹

Reactie CBP: Het CBP begrijpt uit de zienswijze van KPN dat zij een onderscheid maakt tussen direct marketing (verkoopactiviteiten) en marktonderzoek. Artikel 11.5, derde lid, van de Tw vereist echter toestemming van de betrokkenen voor zowel marktonderzoek als verkoopactiviteiten met betrekking tot elektronische communicatiediensten.

³⁷⁷ Zienswijze 1 KPN, p. 69 e.v.

³⁷⁸ Idem.

³⁷⁹ Idem, p. 70-71.

³⁸⁰ Idem.

³⁸¹ Idem, p. 71.

Verder heeft het CBP in dit Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat KPN *niet* rechtmatig over de ‘achterliggende’ gegevens beschikte, zodat het ook niet mogelijk is deze gegevens te anonimiseren en verder te verwerken voor marktonderzoek.

De zienswijze 1 van KPN heeft op het punt van de verdere verwerking geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat omdat KPN niet mag beschikken over de initiële (achterliggende) persoonsgegevens, het KPN ook niet is toegestaan om deze gegevens naderhand te anonimiseren om ze (in geanonimiseerde vorm) verder te verwerken voor marktonderzoek).

Zienswijze 1 KPN: KPN stelt dat het WhatsApp-incident geen impact heeft gehad op de privacy van gebruikers: *“de gegevens zijn niet voor direct marketingdoeleinden gebruikt, konden op geen enkel moment worden gekoppeld door de afdeling [VERTROUWELIJK] aan NAW-gegevens zodat geen daadwerkelijke identificatie plaats heeft kunnen vinden”*.³⁸² Om die reden *“is de Wbp niet van toepassing en kan dit niet als een onzorgvuldige verwerking van persoonsgegevens worden aangemerkt”*, aldus KPN.³⁸³

Reactie CBP: Het CBP heeft in dit Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat de besproken gegevens persoonsgegevens zijn, waarop de Wbp van toepassing is. Het enkele feit dat de gegevens niet zijn gebruikt voor direct marketingdoeleinden, maar voor marktonderzoek maakt dat niet anders. Het CBP heeft in dit Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat KPN geen grondslag had voor de eenmalige verstrekking van persoonsgegevens (tevens verkeersgegevens) over het WhatsApp-gebruik (over de periode februari-april 2011) van alle KPN abonnees met een (postpaid of prepaid) data abonnement aan het KPN retailbedrijf. De gegevensverwerking was (ook) in zoverre niet in overeenstemming met de wet.

De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

³⁸² Zienswijze 1 KPN, p. 70.

³⁸³ Idem, p. 71.

Informatieplicht

Zienswijze 1 KPN: In haar zienswijze betoogt KPN dat de Tw uitputtend de informatieverplichtingen van KPN regelt en dat het CBP niet is belast met het toezicht op de naleving van informatieplichten van telecomaanbieders onder de Tw.³⁸⁴ KPN verwijst daarbij naar artikel 11.3, derde lid, van de Tw dat de aanbieder van een openbare elektronische communicatiedienst of -netwerk (kort gezegd) verplicht ervoor te zorgen dat abonnees worden geïnformeerd over (a) bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst en (b) de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, *voor zover het andere maatregelen betreft dan die welke de aanbieder gehouden is zelf te treffen* op grond van artikel 11.3, eerste lid, van de Tw. Tevens verwijst KPN naar artikel 20 van de Universeledienstrichtlijn (geïmplementeerd in artikel 7.1, eerste en vijfde, lid, van de Tw jo. artikel 3.5b van het BUDE) dat de aanbieder van een openbare elektronische communicatiedienst of -netwerk verplicht informatie op te nemen in het contract met de abonnee over onder andere 'maatregelen om het verkeer te meten en te sturen met als doel te voorkomen dat een netwerkaansluiting tot haar maximum wordt gevuld of overloopt'.

Reactie CBP: De Tw geeft aan bepaalde algemene normen uit artikel 34 van de Wbp een nadere invulling, waaronder in artikel 11.5, vierde lid en artikel 11.2a, derde lid, van de Tw (nieuw). Dit laatste artikel is in werking getreden op 1 januari 2013, na verzending van het Conceptrapport definitieve bevindingen.

De algemene informatieverplichtingen uit hoofde van de Wbp zijn onverkort van toepassing voor die onderdelen die geen uitwerking hebben gekregen in de Tw.³⁸⁵ Artikel 34 van de Wbp heeft in zoverre een aanvullende werking, namelijk voor die onderdelen die niet door de artikelen van de Tw worden gedekt (bijvoorbeeld de verwerking van persoonsgegevens, tevens verkeersgegevens ten behoeve van de overbrenging van communicatie, en de afgeleide doeleinden verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten en opsporing van fraude) (artikel 11.5, eerste en vijfde lid, van de Tw).

Het CBP heeft in dit Conceptrapport definitieve bevindingen vastgesteld dat filtering van uitgaande spam en virus- en malwarebestrijding noodzakelijk is voor (de uitvoering van) de zorgplicht internetveiligheid als bedoeld in artikel 11.3, eerste lid, van de Tw. Artikel 11.3, derde lid, van de Tw heeft daarom geen betrekking op het gebruik van firewalls, spamfilters en virusscanners. Ten aanzien van artikel 7.1, eerste en vijfde, lid, van de Tw jo. artikel 3.5b van het BUDE (nieuw) geldt dat deze transparantieplicht(en) een andere ratio hebben dan artikel 34 van de Wbp. Te weten: het ervoor zorgen dat de abonnee een goed beeld heeft van het aanbod, voordat hij een contract afsluit, zodat hij goede inschatting kan maken van de te verwachten kwaliteit van de dienstverlening (oftewel, het consumentenrechtelijk perspectief) versus de betrokkene in staat stellen te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerken of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten (oftewel, het grondrechtelijke perspectief ter zake van het recht op

³⁸⁴ Idem, p. 22-23 en 72

³⁸⁵ Bijvoorbeeld ten aanzien van persoonsgegevens, tevens communicatie (dat wil zeggen: in elk geval tot de inwerkingtreding van artikel 11.2a Tw (nieuw) op 1 januari 2013).

bescherming van persoonsgegevens en de persoonlijke levenssfeer).³⁸⁶ De bepaling is in zoverre niet uitputtend.

De zienswijze 1 van KPN heeft op het punt van de informatieplicht geleid tot verduidelijking en aanpassing van het toepasselijke en toegepaste wettelijk kader. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat doordat KPN niet informeert over de categorieën van verwerkte persoonsgegevens, tevens communicatie er (nog) sprake is van een overtreding van artikel 34 van de Wbp.

Zienswijze 1 KPN: Onjuist is volgens KPN de bevinding van het CBP dat de passage uit de privacy policies over de verwerking van persoonsgegevens anders dan verkeersgegevens onjuist zijn, omdat KPN op geen enkel moment kennis neemt van de inhoud van communicatie: *“niet bijhoudt welke websites worden bezocht, wat op deze websites staat en geen kennis neemt van inhoud van e-mail en chatberichten.”*³⁸⁷

Reactie CBP: KPN gaat er in haar zienswijze aan voorbij dat zij ook persoonsgegevens, tevens communicatie verzamelt/genereert, gebruikt, vastlegt en bewaart. KPN erkent ook met zoveel woorden hostnames (URL op hoofddomein) en referers (laatst bezochte website) te verwerken. Zij houdt dus wel degelijk bij welke websites worden bezocht.

De zienswijze 1 van KPN heeft op het punt van de informatieplicht geleid tot verduidelijking en aanpassing van het toepasselijke en toegepaste wettelijk kader. De zienswijze 1 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport (de zienswijze 2 van KPN heeft op dit punt wel geleid tot aanpassing van de conclusies).

Zienswijze 1 KPN: KPN geeft in haar zienswijze aan dat het algemene KPN privacy statement ongelukkig is geformuleerd, bijvoorbeeld waar de verkeersgegevens die KPN verwerkt (onder meer de URL van de applicatieserver) worden aangeduid met ‘surfgedrag’.³⁸⁸ KPN verklaart verder dat zij in het licht van de geconstateerde onduidelijkheden en de publieke commotie die is ontstaan rondom de toepassing van data-analyse technieken doende is om de KPN en de Hi privacy statements op een aantal punten aan te vullen en te verduidelijken, en dat zij zodra KPN de nieuwe privacy statements heeft afgerond deze aan het CBP zal doen toekomen. KPN zegt per doeleinde in begrijpelijker taal inzicht te zullen geven in (i) de categorieën

³⁸⁶ “Op basis van deze onderdelen kan worden voorgeschreven dat aanbieders van openbare elektronische communicatiediensten en -netwerken, transparant maken welke beperkingen zij aanbrengen inzake toegang tot of het gebruik van diensten en toepassingen (onderdeel b) en welke maatregelen zij treffen teneinde om te gaan met congestie op het netwerk (het meten en sturen van netwerkverkeer teneinde te voorkomen dat een netwerkaansluiting overloopt) en de gevolgen van deze maatregelen voor de kwaliteit van de dienstverlening (onderdeel d). Voor de consument is het van belang om een goed beeld te hebben van het aanbod, voordat hij een contract afsluit, zodat een goede inschatting kan worden gemaakt van de te verwachten kwaliteit van de dienstverlening. Een verkeersmaatregel heeft in beginsel steeds gevolgen voor de gebruikservaring van verschillende diensten en toepassingen, in het bijzonder bij drukte op het netwerk (congestie).” Nota van toelichting bij het Besluit implementatie herziene telecomunicatierichtlijnen (Stb. 2012, 236, p. 27).

³⁸⁷ Zienswijze 1 KPN, p. 72-73.

³⁸⁸ Idem, p. 72.

verkeersgegevens en/of persoonsgegevens die worden verwerkt, (ii) of de gegevens ten behoeve van het KPN [VERTROUWELIJK] of het KPN retailbedrijf worden verwerkt, (iii) uitleg over hoe KPN het netwerkverkeer meet en stuurt en (iv) hoe lang de betreffende gegevens worden bewaard. KPN verzoekt het CBP de nieuwe privacy policies in haar definitieve bevindingen mee te wegen.³⁸⁹ KPN heeft het CBP op 4 juni 2012 haar nieuwe privacy statements en (kopieën van haar) gewijzigde meldingen verstrekt

Reactie CBP: KPN geeft aan dat zij, zonder aanvaarding van enige gehoudenheid daartoe, aanleiding heeft gezien om haar privacy statements en de meldingen bij het CBP aan te passen. De door KPN doorgevoerde aanpassingen van haar privacy statements verhelpen de geconstateerde overtredingen onvoldoende.

De overtreding van artikel 34 van de Wbp is ten dele beëindigd, nu KPN de doeleinden van de verwerking 'netwerkplanning- en beheer' (daaronder mede begrepen het voorkomen van congestie) en 'het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed' en de categorieën van verwerkte persoonsgegevens, tevens verkeersgegevens alsnog heeft beschreven in haar nieuwe privacy statements. KPN informeert betrokkenen via de tekst uit de nieuwe privacy statements niet over de categorieën van verwerkte persoonsgegevens, tevens communicatie zoals hostnames en referers

De zienswijze 1 van KPN heeft op dit punt in zoverre geleid tot aanpassing van de bevindingen en conclusies in het rapport.

Meldingsplicht

Zienswijze 1 KPN: KPN brengt in haar zienswijze naar voren dat deze wijziging van de melding onverplicht is (gedaan).³⁹⁰

KPN merkt op dat de door haar verwerkte verkeersgegevens geen persoonsgegevens betreffen in de zin van de Wbp en dat voor zover KPN een melding heeft gedaan, dit onverplicht is gedaan. Verder brengt KPN naar voren dat zij niet gehouden is het gebruik van data-analyse op te nemen in de melding omdat dit geen zelfstandig doel is, maar een middel om de beschreven doelen te bereiken. Datzelfde geldt volgens KPN voor het gebruik van firewalls, spamfilters en virusscanners (middelen om netwerkintegriteit en -continuïteit te bereiken). Facturering van prepaidverkeer valt onder het doeleinde facturering, aldus KPN. Niettemin heeft KPN onverplicht de hiervoor genoemde doeleinden in de melding verduidelijkt en de omschrijving van de categorie verkeersgegevens (bijvoorbeeld de begrippen 'gebruiksgegevens', 'surfgedrag' en 'kijkgedrag') aangepast.³⁹¹

Reactie CBP: Het CBP heeft in dit Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat KPN persoonsgegevens verzamelt/verwerkt bij de

³⁸⁹ Idem, p. 73.

³⁹⁰ Idem, p. 75. Zie ook brief KPN van 4 juni 2012, p. 1: "KPN is (overigens al voordat het CBP het onderzoek instelde) een project gestart dat ziet op de heroverweging van het KPN brede privacybeleid."

³⁹¹ Zienswijze 1 KPN, p. 74-75.

inzet van data-analyse technieken in haar mobiele netwerk. Het CBP betoogt niet dat KPN is gehouden de inzet van data-analyse te omschrijven *als doeleinde* bij de melding die zij heeft gedaan. Het CBP heeft hierboven vastgesteld of de doeleinden van de gegevensverwerking die betrekking hebben op de verwerking van persoonsgegevens *bij de inzet van data-analyse technieken in haar mobiele netwerk* die KPN heeft geformuleerd volledig en voldoende duidelijk zijn omschreven in de doelomschrijving in de melding die KPN heeft gedaan. Uit de doelomschrijving 'het factureringsproces, waaronder notanavraag, klachtafhandeling, storingsopheffing, advisering, e.d.' blijkt niet, althans onvoldoende duidelijk dat KPN met behulp van data-analyse technieken het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed faciliteert. Ook uit de doelomschrijving 'netwerkmanagement, waaronder netwerkplanning en netwerkarchitectuur, netwerkindegriteit en fraudedetectie' blijkt niet, althans onvoldoende duidelijk dat KPN firewalls, spamfilters en virusscanners inzet voor netwerkindegriteit en -continuïteit. De overtreding van artikel 7 van de Wbp is inmiddels ten dele beëindigd, nu KPN het doeleinde het gebruik van firewalls, spamfilters en virusscanners inzet voor netwerkindegriteit en -continuïteit alsnog heeft gemeld bij het CBP (dat geldt niet voor het doeleinde het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed).

De zienswijze 1 van KPN heeft op het punt van de melding geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies.

Bijlage VI Zienswijze 2 KPN op de Concept definitieve bevindingen, met de reactie daarop van het CBP (zoals weergegeven in het rapport definitieve bevindingen, gegroepeerd én aangevuld in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van het rapport definitieve bevindingen).

Stopzetten en gestopt houden data-analysetools voor netwerkmanagement en prepaid facturering

Zienswijze 2 KPN: KPN brengt in haar reactie op het Conceptrapport definitieve bevindingen naar voren dat zij heeft besloten de data-analysetools voor netwerkmanagement ([VERTROUWELIJK: apparatuur]) en het afrekenen van prepaidverkeer ([VERTROUWELIJK: apparatuur]) met ingang van 21 september 2012 respectievelijk 3 oktober 2012 stop te zetten en gestopt te houden, behoudens nader tegenbericht. KPN geeft verder (onderbouwd met een verklaring³⁹²) aan alle via de [VERTROUWELIJK: apparatuur] opgeslagen data én de geanonimiseerde [VERTROUWELIJK: apparatuur]-data die zijn verstrekt aan het KPN retailbedrijf voor de analyse van de eigen dienstverlening, te hebben verwijderd per uiterlijk 11 oktober 2012. KPN is daarnaast in overleg getreden met de leverancier van de [VERTROUWELIJK: apparatuur] voor het ontwikkelen en uitbrengen van een technisch alternatief dat ervoor zorgt dat verkeersgegevens zo snel mogelijk omkeerbaar worden geanonimiseerd (KPN acht zo'n alternatief op dit moment proportioneel). Als alternatief voor de data-analyse functionaliteit van de [VERTROUWELIJK: apparatuur] verleent KPN thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK], op zo'n manier dat [VERTROUWELIJK].³⁹³

Reactie CBP: De zienswijze 2 van KPN heeft op dit punt geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies. Door het stopzetten en gestopt houden van de data-analysetool voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) alsmede de verwijdering van de verzamelde en verwerkte [VERTROUWELIJK: apparatuur]-gegevens, worden voor dit hiervoor genoemde doeleinde thans geen persoonsgegevens die ook verkeersgegevens zijn meer verwerkt en handelt KPN (daardoor) niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag). Door aanpassing van de data-analysetool voor het afrekenen van prepaidverkeer ([VERTROUWELIJK: apparatuur]) verleent KPN thans toegang tot (gratis) opwaardeersites op basis van [VERTROUWELIJK] in plaats van op basis van analyse van URL's om daaruit de opwaardeersites te herkennen. Dit is in deze context een proportionele implementatie van het bieden van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed, direct via 'mobiel internet', gelet op de omstandigheid dat de verwerkte gegevens [VERTROUWELIJK] en niet worden opgeslagen en bewaard. Door deze aanpassing handelt KPN niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

³⁹² Bijlage 1 bij reactie KPN op vordering van 28 februari 2013.

³⁹³ Zienswijze 2 KPN, p. 2-5.

Opmerkingen en aanvullingen feitelijk kader

Zienswijze 2 KPN: KPN brengt in haar reactie op het Conceptrapport definitieve bevindingen een aantal opmerkingen en aanvullingen van feitelijke aard naar voren ten aanzien van de werking van de door KPN ingezette data-analyse tools (vóór het stopzetten) en de verwachte groei van het signaleringsverkeer.

KPN geeft, allereerst, (samengevat weergegeven) aan dat of de inzet van data-analysetools impact heeft op de privacy van eindgebruikers afhangt van het doel waarvoor data-analyse wordt toegepast en de wijze waarop de data-analysetools worden ingericht. Data-analysetools ‘zien’ of verwerken niet meer dan dat waarvoor ze zijn ingesteld. De data-analysetools van KPN zijn ingesteld om een beperkt aantal (vooraf gedefinieerde) applicaties te identificeren, waarbij telkens slechts het eerste datapakketje wordt geanalyseerd (van een reeks pakketjes die samen een bericht vormen) op grond van vooraf gedefinieerde kenmerken. Hierbij wordt enkel gekeken naar verkeersgegevens, zoals protocollen en headers. De communicatie-inhoud is niet van belang om te komen tot een succesvolle identificatie. Ook wanneer de gebruiker de inhoud van zijn communicatie zou hebben versleuteld door middel van encryptie (en het derhalve niet mogelijk is om door middel van de data-analysetools de inhoud ‘te lezen’), blijft identificatie van de applicatie mogelijk. Dit betekent dat: (i) wanneer een abonnee geen van de vooraf vastgestelde apps op zijn smartphone heeft staan en gebruikt, de [VERTROUWELIJK: apparatuur] van deze abonnee in het geheel geen gegevens over zijn gebruik verzamelt en opslaat; (ii) wanneer een abonnee wel een vooraf vastgestelde app op zijn smartphone heeft staan en gebruikt, de [VERTROUWELIJK: apparatuur] alleen die gegevens verzamelt en bewaart die nodig zijn om de app te kunnen identificeren (de hoeveelheid en categorieën gegevens die nodig zijn om een bepaalde app te identificeren, verschilt per app).³⁹⁴

KPN merkt verder op dat het CBP in het Conceptrapport definitieve bevindingen onder verwijzing naar een citaat van het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, stelt dat de toename van het datavolume dient te worden gerelativeerd. Volgens KPN slaat de relativering door BEREC louter op de toename in dataverkeer (aantallen bytes) en is deze (daarom) niet toepasbaar op de ongekende groei die KPN ervaart in het signaleringsverkeer (aantallen signaleringen) dat over haar mobiele netwerk gaat. KPN erkent dat de groei van dataverkeer, hoewel een uitdaging, van een andere orde is.³⁹⁵

KPN benadrukt daarnaast, onder verwijzing naar berichtgeving in de media over ernstige verstoringen in het mobiele netwerk van twee andere Europese telecommunicatieaanbieders in verband met signaleringsverkeer, groeiprognozes van [VERTROUWELIJK] (gemiddeld groeipercentage van 252%, verwacht groeipercentage voor Europa van 320% per jaar) en de aandacht in het nieuws die verstoringen in het netwerk van Nederlandse telecommunicatieaanbieders krijgen, dat de impact die het toegenomen signaleringsverkeer wereldwijd heeft op mobiele netwerken van telecommunicatieaanbieders actueel blijft.³⁹⁶ Het besluit tot stopzetten van de inzet van de [VERTROUWELIJK: apparatuur] voor het meten van het

³⁹⁴ Idem, p. 7-8.

³⁹⁵ Idem, p. 9.

³⁹⁶ Idem, p. 10-12.

signaleringsverkeer heeft (daarom) potentieel impact op het functioneren van het mobiele netwerk van KPN, dat ten opzichte van het vaste netwerk steeds belangrijker wordt.³⁹⁷

Volgens KPN doet, ten slotte, het feit dat er naast het uitbreiden van de (signalerings)capaciteit in het mobiele netwerk ook andere initiatieven (samenwerkingsprojecten met producten van smartphone besturingssystemen en apps) bestaan om de druk op het signaleringskanaal te verminderen, niets af aan het voorgaande. Dit omdat (i) het langere termijn initiatieven zijn die tot nu toe niet hebben geleid tot concrete oplossingen, (ii) het slagen van zulke samenwerkingsprojecten afhankelijk is van de medewerking van producten van smartphone besturingssystemen en apps die een tegengesteld belang hebben aan dat van de telecommunicatieaanbieders (een chatty app draagt bij aan de gebruiksbeleving), terwijl (iii) KPN compleet afhankelijk van de goodwill van deze ontwikkelaars - die niet centraal zijn georganiseerd - omdat zij geen enkel juridisch middel heeft om de ontwikkeling van minder netwerk belastende apps af te dwingen.³⁹⁸

Reactie CBP: De zienswijze 2 van KPN heeft op het punt van de werking van de door KPN ingezette data-analysetools (vóór het stopzetten/aanpassen daarvan) geleid tot verduidelijking en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 2 van KPN heeft op het punt van de verwachte groei van het signaleringsverkeer geleid tot enerzijds verduidelijking in de feitelijke bevindingen in het rapport van de impact die het toegenomen signaleringsverkeer heeft op het mobiele netwerk van KPN en anderzijds nuancering van het belang van (i) de relativisering door BEREK van de toename in dataverkeer en (ii) andere initiatieven om de druk op het signaleringskanaal te verminderen. De zienswijze 2 van KPN heeft op deze punten evenwel niet geleid tot aanpassing van de conclusies in het rapport (want het betreffen geen dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat een alternatief voor de door KPN ingezette data-analysetool voor netwerkplanning en -beheer dat ervoor zorgt dat verkeersgegevens zo snel mogelijk onomkeerbaar worden geanonimiseerd op dit moment proportioneel is).

Bevoegdheid CBP

Zienswijze 2 KPN: KPN betoogt in haar reactie op het Conceptrapport definitieve bevindingen dat het CBP slechts bevoegd is om de bepalingen van hoofdstuk 11 van de Tw toe te passen voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie. Het is het CBP niet toegestaan om buiten hoofdstuk 11 en 13 van de Tw (de implementatie van de e-Privacyrichtlijn en de Dataretentierichtlijn 2006/24/EG) toe te zien op andere bepalingen uit de Tw. Voor zover het CBP in het Conceptrapport definitieve bevindingen een oordeel geeft over artikel 7.4a van de Tw (nieuw), treedt het CBP buiten haar bevoegdheid. Doel en strekking van dit artikel 7.4a van de Tw is het waarborgen van de vrije toegankelijkheid van het internet en het ervoor zorgdragen dat bedrijven en consumenten vrijelijk gebruik kunnen maken van internet als communicatiemiddel,

³⁹⁷ Idem, p. 10 en 13.

³⁹⁸ Idem, p. 12-13.

niet de bescherming van persoonsgegevens, waardoor het toezicht op dit artikel uitsluitend zal berusten bij OPTA (nu: ACM).³⁹⁹

Reactie CBP: Het CBP is, zoals KPN betoogt, (inderdaad) slechts bevoegd toe te zien op (onder meer) de naleving van de bepalingen van de Wbp en van hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie. Anders dan KPN lijkt te argumenteren, loopt het CBP niet vooruit op/geeft het CBP geen oordeel over *de naleving door KPN* van artikel 7.4a van de Tw. Wel kan de uitleg van artikel 7.4a van de Tw relevant zijn voor de vraag of er voor KPN een wettelijke plicht (grondslag) is voor de verwerking van niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn voor het doeleinde van netwerkplanning en -beheer. Artikel 7.4a van de Tw (nieuw) regelt de verplichting voor aanbieders om netneutraal te handelen, met daarop een aantal uitzonderingen (bijvoorbeeld om de gevolgen van congestie te beperken, waarbij gelijke soorten verkeer gelijk worden behandeld, of ter uitvoering van een wettelijk voorschrift of rechterlijk bevel). Het CBP heeft de uitleg van de wet, dat artikel 7.4a van de Tw (dus) op zichzelf geen grondslag geeft voor de verwerking van niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn (maar uitzonderingen op de netneutraliteitsverplichting), (nogmaals) voorgelegd aan ACM in het kader van het Samenwerkingsprotocol CBP-OPTA.⁴⁰⁰ ACM, de ter zake bevoegde toezichthouder, stemt in met deze voorgelegde toepassing van dit wetsartikel.

De zienswijze 2 van KPN heeft op het punt van de bevoegdheid van het CBP geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Samenloop Wbp en Tw: grondslagtoetsing

Zienswijze 2 KPN: KPN stelt zich in haar reactie op het Conceptrapport definitieve bevindingen op het standpunt dat het CBP voor zijn beoordeling van de geconstateerde overtredingen telkens de grondslagen uit de Wbp als uitgangspunt neemt en niet de grondslagen die voor de betreffende verwerkingen in de Tw zijn gegeven, terwijl:

- uit de Europese wetgeving blijkt dat de Privacyrichtlijn alleen geldt in die gevallen waarin de e-Privacyrichtlijn geen specifieke regeling bevat;⁴⁰¹
- de wetsgeschiedenis bij de Wbp en de Tw uitdrukkelijk stelt dat de Tw op onderdelen een *specialis* is ten opzichte van de Wbp;⁴⁰²
- artikel 11.5 van de Tw (aldus) een uitputtende regeling geeft voor de verwerking van verkeersgegevens die ook persoonsgegevens zijn;⁴⁰³ en

³⁹⁹ Idem, p. 14-16.

⁴⁰⁰ Vgl. ook considerans 2 van het Samenwerkingsprotocol CBP-OPTA: “Dit document geeft de afspraken weer over de wijze van behandeling van aangelegenheden waarbij de aan OPTA en het CBP opgedragen taken of de uitoefening van de aan OPTA en het CBP toegekende bevoegdheden elkaar raken of overlappen”, (onderstreping toegevoegd door het CBP).

⁴⁰¹ Idem, p. 17-19.

⁴⁰² Idem, p. 19-26.

⁴⁰³ Idem, p. 26-28.

- de verwerking van communicatie voor beveiligingsdoeleinden en netwerkmanagement ook uitputtend is geregeld in artikel 11.3 en/of artikel 11.2a Tw (nieuw) van de Tw.⁴⁰⁴

KPN geeft in haar reactie op het Conceptrapport definitieve bevindingen ook aan dat toetsing aan louter de grondslagen in de Tw, zoals voorgestaan door KPN, (op een enkel onderdeel na) niet leidt tot een drastisch andere uitkomst dan *“de toetsing door het CBP aan de grondslagen in de Wbp”*.⁴⁰⁵

Reactie CBP: Het CBP wijst erop dat de e-Privacyrichtlijn (geïmplementeerd in de Tw) zich verhoudt tot de Privacyrichtlijn (geïmplementeerd in de Wbp) als sectorale tot algemene regels.⁴⁰⁶ De richtlijnen hebben (deels) een ander karakter⁴⁰⁷ en een ander toepassingsbereik. Dat wil zeggen dat - anders dan de Privacyrichtlijn - de e-Privacyrichtlijn ook van toepassing is op de verwerking van verkeersgegevens die geen persoonsgegevens zijn (gegevens van rechtspersonen). Anders dan de e-Privacyrichtlijn, geldt de Privacyrichtlijn ook voor zover het gaat om de verwerking van verkeersgegevens die ook persoonsgegevens zijn in niet openbare elektronische communicatienetwerken en -diensten. Op dezelfde manier is de verhouding tussen de Tw en de Wbp er een van (aanvullende) sectorale normen naast - en niet in plaats van - de Wbp.⁴⁰⁸ Er is in algemene zin geen sprake van een lex specialis-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene. Wel geldt dat indien en voor zover de e-Privacyrichtlijn (als geïmplementeerd in de Tw) ten aanzien van de verwerking van persoonsgegevens op een bepaald punt een uitputtende regeling bevat, die regeling voorgaat op de algemene normen uit de Privacyrichtlijn (als geïmplementeerd in de Wbp).⁴⁰⁹

Artikel 11.5 van de Tw vormt een implementatie van artikel 6 van de e-Privacyrichtlijn en geeft regels voor de verwerking van verkeersgegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten. Uit de wetsgeschiedenis bij de Tw blijkt dat artikel 11.5 van de Tw, zoals KPN betoogt, (inderdaad) is bedoeld als uitputtende regeling: *“In artikel 11.5 van de wet worden aan de verwerking van verkeersgegevens specifieke voorwaarden gesteld en voor zover het daarbij gaat*

⁴⁰⁴ Idem, p. 28-43.

⁴⁰⁵ Idem, p. 4.

⁴⁰⁶ Uit de tekst van artikel 3, eerste lid, van de Privacyrichtlijn volgt dat deze een algemeen - niet sectoraal - toepassingsbereik heeft. De algemene Privacyrichtlijn is daarom mede van toepassing op de verwerking van persoonsgegevens in de telecommunicatiesector. Zie ook *Kamerstukken II 1996/97*, 25 533, nr. 3, p. 13. Uit de tekst van artikel 1, tweede lid, van de telecomspecifieke e-Privacyrichtlijn volgt dat de bepalingen van deze richtlijn ‘een specificatie van en een aanvulling’ vormen op de Privacyrichtlijn. Zie in dezelfde zin overweging 10, 12, 20, laatste volzin, en 46 en artikel 4, eerste lid bis, van de e-Privacyrichtlijn.

⁴⁰⁷ Bijvoorbeeld: de bepalingen in de e-Privacyrichtlijn die betrekking hebben op de beschikbaarheid van nummeridentificatie. Vgl. *Kamerstukken II 2002/03*, 28 851, nr. 7, p. 54.

⁴⁰⁸ *Kamerstukken II 1999/2000*, 26 410, nr. 7, p. 2. Zie in dat verband ook *Kamerstukken II 2002/03*, 28 851, nr. 7, p. 78-79.

⁴⁰⁹ Zie ook *Kamerstukken II 2002/03*, 28 851, nr. 3, p. 45.

om de verwerking van persoonsgegevens dienen die als een specialis ten opzichte van de algemene normen uit de Wbp ter zake te worden aangemerkt.”⁴¹⁰

Voor het verwerken van persoonsgegevens is (desondanks) een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8 van de Wbp. Uit de wetsgeschiedenis bij de Wbp kan wel worden afgeleid dat artikel 8 van de Wbp een uitputtende opsomming geeft van verwerkingsgronden: *“Artikel 7 betreft de verzameling van persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Hierop zijn geen uitzonderingen. Hetzelfde geldt voor de in artikel 8 genoemde gronden op basis waarvan persoonsgegevens mogen worden verwerkt. Artikel 8 omvat derhalve een uitputtende opsomming van verwerkingsgronden.”⁴¹¹*

Als hoofdregel geldt op grond van dit artikel 11.5 van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor facturering, of voor marktonderzoek/verkoopactiviteiten en toegevoegde waardediensten mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor toestemming heeft gegeven).

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp⁴¹² op het punt van de bevoegdheid tot (toelaatbaarheid van) het bewaren van persoonsgegevens die ook verkeersgegevens zijn (oftewel, een verplichting tot verwijdering dan wel anonimisering van gegevens, met uitzonderingen).⁴¹³ Dit artikel geeft echter op zichzelf geen grondslag voor de verwerking van de niet verwijderde of niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn (maar uitzonderingen op de verwijderings-/anonimiseringsplicht).⁴¹⁴ Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) doeleinden,

⁴¹⁰ *Kamerstukken II 2002/03, 28 851, nr. 7, p. 54. Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 59.*

1998/99, 25 892, nr. 13, p. 5-6.

aard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

p. 27.

⁴¹⁴ *Vgl. de verbods- en ontheffingssystematiek ten aanzien van de verwerking van bijzondere persoonsgegevens (artikel 16 e.v. van de Wbp). In de wetsgeschiedenis bij de Wbp is daarover het volgende opgemerkt “Artikel 16 is conform de richtlijn geformuleerd als een verbod. Dit impliceert dat als hoofdregel geldt dat verwerking van gevoelige gegevens niet is toegestaan. De daarop volgende bepalingen (artikel 17 tot en met 23) zijn in dezelfde sleutel geplaatst en geformuleerd als een ontheffing van het algemene verwerkingsverbod. Langs deze weg wordt ook tot uitdrukking gebracht dat artikel 17 e.v. niet zonder meer legitimeren tot gegevensverwerking: zij doorbreken slechts een verbod. Vervolgens zal aan de hand van de algemene beginselen van gegevensverwerking - zoals vastgelegd in artikel 6 tot en met 15 van het wetsvoorstel - moeten worden vastgesteld of de gegevensverwerking in het concrete geval rechtmatig is”, (onderstreping toegevoegd door het CBP). *Kamerstukken II 1997/98, 25 892, nr. 3, p. 101.**

dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp.

Wel geeft de uitputtende regeling in artikel 11.5 van de Tw een nadere begrenzing/inperking van de toegestane verwerkingen van persoonsgegevens die ook verkeersgegevens zijn in de telecommunicatiesector, namelijk waar het gaat om de vraag of (lees: hoe lang) een grondslag is te vinden in de Wbp voor de verwerking van niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn. Het CBP heeft de beoordeling van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn derhalve getoetst aan artikel 11.5 van de Tw jo. artikel 8 van de Wbp. Dat betekent materieel (inhoudelijk) dat als de gegevensverwerking is toegestaan onder artikel 11.5 van de Tw ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de Tw ook geen grondslag is te vinden in de Wbp.

Ten aanzien van de verwerking van communicatie, tevens persoonsgegevens geldt het volgende.

Artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) geeft een verplichting voor de aanbieders van openbare elektronische communicatienetwerken en -diensten om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Dit artikel stelt eisen aan de beveiliging van persoonsgegevens en geeft aldus een telecomspecifieke uitwerking van artikel 13 van de Wbp.⁴¹⁵ Het artikel geeft (dus) op zichzelf geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

Artikel 5 van de e-Privacyrichtlijn regelt het vertrouwelijk karakter van de communicatie. Als hoofdregel geldt op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers verboden is, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit artikel geeft aldus een verwerkingsverbod, met uitzonderingen (zij doorbreken slechts een verbod). Op deze eerder genoemde hoofdregel is in lid 2 van artikel 11.2a van de Tw bijvoorbeeld een uitzondering geformuleerd voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder. Het artikel geeft echter op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens (maar uitzonderingen op het verwerkingsverbod).

Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.3 en/of artikel 11.2a van de Tw

⁴¹⁵ Te weten: het vereiste dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (beveiliging). Vgl. T&C Telecommunicatierecht, commentaar op artikel 11.3 Telecommunicatiewet en T&C Telecommunicatierecht, commentaar op artikel 13 WBP.

genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Dat daargelaten, geeft de regeling in artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) een nadere begrenzing/inperking van de toegestane verwerkingen van persoonsgegevens die ook communicatie betreffen in de telecommunicatiesector, namelijk waar het gaat om de vraag of daarvoor een grondslag is te vinden in de Wbp. Het CBP heeft de beoordeling van de grondslag voor het verwerken van persoonsgegevens die ook communicatie betreffen derhalve getoetst aan artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp. Dat betekent materieel (inhoudelijk) dat als de gegevensverwerking is toegestaan onder artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw ook geen grondslag is te vinden in de Wbp.

De zienswijze 2 van KPN heeft op het punt van de samenloop van Wbp en Tw, meer in het bijzonder de toetsing van de grondslag voor (i) de verwerking van persoonsgegevens die ook verkeersgegevens zijn en (ii) de verwerking van communicatie, tevens persoonsgegevens, geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van KPN heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Onderscheid verkeersgegevens en communicatie

Zienswijze 2 KPN: KPN betoogt in haar reactie op het Conceptrapport definitieve bevindingen (nogmaals) dat hoewel de afbakening tussen de termen “communicatie” en “verkeersgegevens” wordt bemoeilijkt door de steeds sterkere vervlechting tussen de gevoerde communicatie en daarmee samenhangende gegevens in de technische protocollen (het http-protocol bevat zowel inhoudskenmerken als verkeersgegevens), dit echter niet betekent dat zodra een verkeersgegeven ook ‘inhoudskenmerken’ bevat, dit per definitie ook communicatie betreft. Het uitgangspunt van de Tw is dat als iets een verkeersgegeven betreft, het regime voor verwerking van verkeersgegevens geldt, ongeacht of het betreffende verkeersgegeven ook inhoudskenmerken bevat. Dit toetsingskader is met name voor URL's (waaronder mede begrepen hostnames en referers) van belang, omdat hieruit volgt dat URL's verkeersgegevens zijn en niet tevens communicatie (KPN monitort/monitorde geen communicatie, anders gezegd: leest geen e-mails, luistert geen telefoons af etc.).⁴¹⁶

KPN merkt daarnaast op dat voor zover URL's werden geanalyseerd bij de inzet van de data-analysetool voor netwerkmanagement (vóór het stopzetten daarvan), alleen de URL's van een zeer beperkt aantal applicatieservers werden ‘gezocht’ (en dus niet de URL's van webpagina's zelf die vaak meer relevante informatie leveren over de inhoud van communicatie, nu deze nagenoeg ook altijd informatie verschaffen over

⁴¹⁶ Zienswijze 2 KPN, p. 44-60.

de betreffende pagina van de website die wordt bezocht, omdat dit de indexatie van zoekmachines bevordert.⁴¹⁷

Reactie CBP: Het CBP volgt KPN in haar standpunt dat het toetsingskader voor de verwerking van URL's (waaronder mede begrepen hostnames en referers) het regime voor verwerking van verkeersgegevens is (oftewel, artikel 11.5 van de Tw jo. artikel 8 van de Wbp). De zienswijze 2 van KPN heeft op het punt van het toetsingskader voor de verwerking van URL's geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport.

Dit mede omdat signature based data analyse ten behoeve van protocol of appherkenning (zoals voip, p2p, of specifieke apps als Skype) plaatsvindt in de initiatiefase van een protocol, bij het opzetten van de verbinding.

In de initiatiefase van een applicatieprotocol worden over het algemeen gegevens vervoerd die nodig zijn om de communicatie tot stand te brengen. Dat daartoe via het TCP en IP protocol uit de onderliggende internet- en transportlagen ook al packets worden vervoerd die gegevens uit de applicatielaag bevatten, betekent niet dat die pakketten dus communicatiegegevens bevatten.

Omdat het niet mogelijk is om vooraf te bepalen wanneer de initiatiefase begint, zullen in beginsel alle headers en de eerste paar packets vergeleken worden met de signature. Op het moment dat er een match is tussen een signature en een packet, is het niet meer nodig om verder te vergelijken. Gelet op het voorgaande worden deze gegevens beoordeeld als verkeersgegevens, tevens persoonsgegevens.

Dit neemt niet weg dat omdat verkeersgegevens veel over de gebruiker kunnen zeggen en raken aan de telecommunicatievrijheid, verkeersgegevens die ook persoonsgegevens zijn ook wel worden aangeduid als gegevens van gevoelige aard.⁴¹⁸ Het CBP wijst er in dat verband verder op dat zowel de inhoud van, als 'informatie over elektronische communicatie' (oftewel, verkeersgegevens) gegevens zijn die bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (Handvest).⁴¹⁹

Overige opmerkingen mogelijke grondslagen voor de inzet van data-analysertools voor prepaid facturering en inkomende spam

Zienswijze 2 KPN: KPN stelt zich in haar reactie op het Conceptrapport definitieve

⁴¹⁷ Idem, p. 53-54.

⁴¹⁸ Vgl. *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. Zie ook idem, nr. 1, p. 27: "(...) het feit dat verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens (...)." Zie ook *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.

⁴¹⁹ Zie o.a. EHRM 3 april 2007, NJ 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44; EHRM 2 augustus 1984, NJ 1988, 534 (Malone) en EHRM 25 september 2001, NJ 2003, 670 (P.G. en J.H./Verenigd Koninkrijk). Het CBP heeft (daarom) in zijn wetgevingsadvies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet geadviseerd nadere aandacht te schenken aan de reikwijdte van het voorgestelde artikel 13 van de Grondwet (de uitzondering voor verkeersgegevens).

bevindingen op het standpunt dat het faciliteren van opwaardeermogelijkheden géén verkoopactiviteit betreft in de zin van artikel 11.5, derde lid, onder a, van de Tw en dat voor het blokkeren van inkomende spam op grond van artikel 7.4a van de Tw géén ondubbelzinnige toestemming nodig is. Dit ook om te voorkomen dat deze stellingen van het CBP tot misverstanden zouden leiden in het vervolg van de procedure dan wel formele rechtskracht zouden krijgen.⁴²⁰

KPN geeft aan dat prepaid klanten (wel) abonnees zijn waarmee KPN één doorlopend contract heeft. De Tw staat toe dat verkeersgegevens worden verwerkt voor facturering. Onder facturering dient ook het registreren van het beltegoed van prepaid klanten te worden begrepen. Hieronder wordt ook begrepen het routeren van verkeer naar opwaardeersites voor opwaardering (het verwerkingsdoel facturering wordt ruim opgevat). Niet begrijpelijk is volgens KPN het oordeel van het CBP dat het doorleiden van gebruikers naar opwaardeersites voor opwaardering van hun beltegoed als een verkoopactiviteit zou hebben te gelden (er wordt niets verkocht in de zin dat er een nieuwe overeenkomst wordt aangegaan). De reden voor stopzetting van KPN van de inzet van de data-analysetool voor de routing van verkeer naar opwaardeersites is (dan ook) niet gelegen in het feit dat dergelijke routing niet is goorloofd, maar omdat KPN heeft ingezien dat een dergelijke routing op een voor de gebruiker minder ingrijpende wijze kon worden gerealiseerd.⁴²¹

Uitsluitend subsidiair (omdat het CBP niet bevoegd is toe te zien op uitleg en naleving van artikel 7.4a van de Tw) betoogt KPN dat (anders dan het CBP concludeert) artikel 7.4a van de Tw niet inhoudt dat uitdrukkelijke toestemming (in de zin van artikel 1, aanhef en onder i, van de Wbp) is vereist voor het filteren van inkomende spam. ‘Gewone toestemming’ in de zin van artikel 3:33 en 3:35 van het Burgerlijk Wetboek (te weten: een op een rechtsgevolg gerichte wilsverklaring) is afdoende. ‘Uitdrukkelijke toestemming’ geldt alleen voor bepalingen uit de e-Privacyrichtlijn (zoals geïmplementeerd in hoofdstuk 11 van de Tw) en niet voor artikel 7.4a van de Tw. KPN merkt op dat in de wetsgeschiedenis is aangegeven dat telecommunicatieaanbieders generiek (en dus niet op basis van individuele opt-ins) moeten kunnen filteren op inkomende spam. In dat geval dienen telecommunicatieaanbieders de toestemming te presenteren als een noodzakelijke voorwaarde voor de te sluiten telecomovereenkomst (wat bijvoorbeeld kan worden bereikt door deze op te nemen in de algemene voorwaarden).⁴²²

Reactie CBP: Volgens Van Dale (Van Dale Groot woordenboek van de Nederlandse taal) betekent de term “factureren” een factuur of facturen opmaken (van -) of op een factuur vermelden. Uit de wetsgeschiedenis bij de Tw volgt (inderdaad) dat het verwerkingsdoel facturering, genoemd in artikel 11.5, tweede lid, van de Tw, ‘ruim’ dient te worden opgevat in de zin dat verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed (dit laatste dient onder facturering te worden begrepen).⁴²³ Dit verwerkingsdoel

⁴²⁰ Zienswijze 2 KPN, p. 60.

⁴²¹ Idem, p. 60-66.

⁴²² Idem, p. 66-71.

⁴²³ *Kamerstukken II* 2002/03, 28 851, nr. 13, p. 20.

correspondeert met de grondslag uitvoering van een overeenkomst en - mogelijk - noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

De enkele omstandigheid dat onder de verwerking ten behoeve van de facturering niet alleen wordt verstaan het opstellen van een factuur, maar ook het afwaarderen van het prepaidtegoed bij gebruik van de prepaidaansluiting met de verschuldigde vergoedingen en het bijhouden van het tegoed (het betreft immers vooruitbetaald(e) kaarten/gebruiksrechten, als het prepaidtegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante dienst (nog) te gebruiken), maakt niet dat het bieden van de mogelijkheid om nieuw tegoed te kopen daar ook zonder meer onder valt. Het faciliteren van opwaardeermogelijkheden is in beginsel - naar zijn aard - veeleer een verkoopactiviteit in de zin van artikel 11.5, derde lid, van de Tw waarvoor toestemming is vereist (die bij opwaardering een betalingsverplichting in het leven roept wat (wederom) noodzaakt tot het bijhouden van het tegoed). Volgens Van Dale betekent de term “verkopen” voor geld, tegen een bepaalde prijs, aan een ander overdoen, vooral om winst te maken, als beroep.

Op grond van haar algemene voorwaarden ‘Algemene voorwaarden en aanvullende voorwaarden voor mobiele telecommunicatiediensten 2012’ heeft KPN (evenwel) een resultaatsverplichting om opwaardeermogelijkheden te bieden. Ofschoon uit deze algemene voorwaarden niet met zoveel woorden blijkt dat KPN zich heeft verbonden om bij een ontoereikend prepaid tegoed (ook) via ‘mobiel internet’ opwaardeermogelijkheden te bieden (om te voorkomen dat de betrokken abonnee zijn prepaidtegoed alsdan alleen kan opwaarderen via bijvoorbeeld een andere, ‘vaste’ internetverbinding), volgt hieruit dat de verwerking van gegevens om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor de facturering. Een abonnee verwacht dit ook.

Het CBP heeft deze uitleg van de wet, dat het faciliteren van opwaardeermogelijkheden op het eerste gezicht wellicht een verkoopactiviteit lijkt waarvoor toestemming is vereist, maar gelet op de resultaatsverplichting om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor het ruime verwerkingsdoel facturering, (nogmaals) voorgelegd aan het Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom - CBP. Agentschap Telecom stemt in met deze voorgelegde toepassing van dit wetsartikel.

Op 1 januari 2013 is artikel 7.4a van de Tw in werking getreden. Artikel 7.4a, eerste lid, aanhef en onder c, van de Tw regelt een toestemmingsvereiste voor het filteren op inkomende spam. In de wetsgeschiedenis bij de Tw is daarover opgemerkt: *“Daarnaast kan het generiek filteren van inkomende spam nuttig zijn omdat klanten dit op prijs stellen en omdat het onnodige belasting van netwerken en systemen voorkomt. Artikel 7.4a, eerste lid, onderdeel c, stelt hiervoor wel als voorwaarde dat de abonnee toestemming heeft gegeven. De aanbieder die alleen generiek op spam wil filteren, zou ervoor kunnen kiezen om bij het afsluiten van een overeenkomst te wijzen op het nut van een spamfilter en het geven van toestemming als voorwaarde voor het sluiten van de overeenkomst te stellen.”*⁴²⁴

⁴²⁴ Kamerstukken I 2011/12, 32 549, G, p. 8.

Het Samenwerkingsprotocol CBP-OPTA (zijnde werkafspraken tussen de verschillende toezichthouders binnen de grenzen van de onderscheidene wetten waarin hun bevoegdheden zijn geregeld) regelt/geeft onder andere bepalingen over de behandeling bij samenlopende bevoegdheden en de uitwisseling en verstrekking van informatie tussen ACM en het CBP. Op grond van artikel 2, tweede en derde lid, van het Samenwerkingsprotocol CBP-OPTA zal de ACM zich bij het uitoefenen van haar bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van de bepalingen van de Tw ligt en zal het CBP zich bij het uitoefenen van zijn bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van bepalingen van de Wbp ligt. Het beoordelen van (een grondslag voor) het filteren op inkomende spam ligt volgens de toezichthouders vanaf de inwerkingtreding van artikel 7.4a van de Tw meer op de weg van de ACM.⁴²⁵ De inzet van data-analyse technieken vanaf 1 januari 2013 voor het filteren op inkomende spam valt daarom buiten de scope van dit onderzoek.

De zienswijze 2 van KPN heeft op het punt van het faciliteren van toegang tot (gratis) opwaardeersites en het toestemmingsvereiste voor het filteren op inkomende spam geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport.

Overtredingen die zijn gestaakt door stopzetten en gestopt houden data-analysetools voor netwerkmanagement en prepaid facturering: grondslag verdere verwerking, informatieplicht, doelomschrijving en meldingsplicht

Zienswijze 2 KPN: KPN brengt in haar reactie op het Conceptrapport definitieve bevindingen naar voren dat nu KPN de data-analysetools voor netwerkmanagement en het afrekenen van prepaidverkeer heeft stopgezet, (daarmee) ook de overige door het CBP geconstateerde overtredingen zijn gestaakt. Het gaat hier om:

- het op geanonimiseerde basis verstrekken aan het KPN retailbedrijf van de gegevens die zij door middel van de inzet van de [VERTROUWELIJK: apparatuur] heeft verzameld voor analyse van haar dienstverlening (niet zijnde marketing in de zin van verkoopactiviteiten)⁴²⁶
KPN maakt daarbij (onder verwijzing naar haar eerdere zienswijze 1) nogmaals bezwaar tegen het labelen van de verdere verwerking ten behoeve van analyse van de eigen dienstverlening als voor marketingdoeleinden.⁴²⁷
- het niet informeren in haar privacy statements over de verwerking van URL's: KPN is, zoals vermeld, (verder) van mening dat URL's geen communicatie betreffen. Ook daaruit volgt (los van het stopzetten van de data-analysetools) dat KPN klanten niet nader hoeft te informeren over de verwerking van URL's. KPN geeft aan het oordeel van het CBP op dit verweer af te wachten alvorens haar privacy statements op dit punt aan te passen.⁴²⁸

⁴²⁵ Vgl. ook de taakverdeling ten aanzien van spam (artikel 5 van het Samenwerkingsprotocol CBP-OPTA). Het artikel geeft op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens, maar uitzonderingen op het verwerkingsverbod.

⁴²⁶ Zienswijze 2 KPN, p. 72-73.

⁴²⁷ Zie o.a. idem, p. 72-73.

⁴²⁸ Idem, p. 73-74.

- het onvolledig en onvoldoende duidelijk in haar melding hebben omschreven dat KPN een data-analysetool inzet voor het faciliteren van toegang tot (gratis) opwaardeersites:

Doordat KPN de inzet van de URL-detectiefunctie van de [VERTROUWELIJK: apparatuur] heeft gedeconfigureerd (waardoor deze niet meer beschikbaar is) en niet meer zal her-installeren, zet KPN voor dit doeleinde geen data-analysefunctionaliteit meer in. KPN verleent thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK]. Hiermee verloopt het faciliteren van toegang tot (gratis) opwaardeersites via [VERTROUWELIJK].

Reactie CBP: De zienswijze 2 van KPN heeft op dit punt geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies. Door het stopzetten en gestopt houden dan wel aanpassen van de data-analysetools voor netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur]) en het faciliteren van toegang tot (gratis) opwaardeersites ([VERTROUWELIJK: apparatuur]) zijn ook de overige door het CBP geconstateerde overtredingen beëindigd. KPN handelt (daardoor) niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag verdere verwerking), artikel 34 van de Wbp (informatieplicht) en artikel 7 jo. 27 en 28 van de Wbp (doelomschrijving en meldingsplicht). Dit nog daargelaten dat het CBP, zoals vermeld, KPN volgt in haar standpunt dat het toetsingskader voor de verwerking van URL's (waaronder mede begrepen hostnames en referers) het regime voor verwerking van verkeersgegevens is en dat KPN betrokkenen reeds daarom niet nader en aanvullend hoeft te informeren over de verwerking van URL's (informatieplicht). Ten slotte heeft het CBP de kwalificatie van de verdere verwerking ten behoeve van analyse van de eigen dienstverlening als 'voor marketingdoeleinden' aangepast in 'voor marktonderzoek (analyse van de eigen dienstverlening)'. Dit om te verduidelijken dat KPN klantgegevens, verkregen met data-analysetools, **niet** heeft gebruikt om klanten met (direct) marketinguitingen te benaderen.

Technisch alternatief [VERTROUWELIJK] dat verkeersgegevens onomkeerbaar anonimiseert

Zienswijze 2 KPN: KPN heeft het CBP op 6, 15 en 28 februari 2013 nadere inlichtingen verstrekt omtrent de door [VERTROUWELIJK] geoffreerde en door KPN voorgestelde anonimiseringsoplossing voor de data-analysetool voor netwerkmanagement ([VERTROUWELIJK: apparatuur]) die KPN voornemens is te implementeren, waarin (samengevat weergegeven) [VERTROUWELIJK] om op een minst ingrijpende manier voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer te kunnen komen tot statistisch betrouwbare analyses van trends in haar mobiele netwerk. KPN heeft daarbij toegezegd (aanvullende) technische en organisatorische waarborgen te treffen om de risico's op heridentificatie te minimaliseren en doelbinding te garanderen (waaronder [VERTROUWELIJK]).⁴²⁹ [VERTROUWELIJK] De totale ontwikkel- en licentiekosten van de [VERTROUWELIJK: apparatuur] zijn in de periode tot 30 juni 2013 in totaal [VERTROUWELIJK].⁴³⁰ Naar verwachting wordt de nieuwe versie van de software op 1 juni 2013 in gebruik genomen.

⁴²⁹ Reactie KPN verzoek om inlichtingen van 6 en 15 februari 2013. Reactie KPN op vordering van 28 februari 2013.

⁴³⁰ Reactie KPN verzoek om inlichtingen van 15 februari 2013, p. 11-12.

KPN geeft ten slotte aan voornemens te zijn (ook) een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-omgeving in te richten om - ondanks de anonimiseringsoplossing - klantklachten over te hoge rekeningen op te kunnen lossen.⁴³¹

Reactie CBP: Na het verstrijken van de 24-uurs periode zijn de [VERTROUWELIJK] gegevens in beginsel niet meer herleidbaar tot een identificeerbare natuurlijke persoon, niet door KPN en niet door een derde. Tot dat moment zijn het persoonsgegevens die ook verkeersgegevens zijn, voor de verwerking waarvan een grondslag is vereist. Het CBP acht het aannemelijk dat het voor KPN noodzakelijk is om op basis van een zo groot mogelijke steekproef, gedurende 24 uur niet geanonimiseerde verkeersgegevens die ook persoonsgegevens zijn te verwerken voor het doeleinde van netwerkplanning en -beheer om te kunnen komen tot statistisch betrouwbare analyses van (acute) trends in het mobiele netwerk. Op basis van het beschikbare onderzoeksmateriaal constateert het CBP, mits KPN op adequate wijze de risico's op heridentificatie minimaliseert en doelbinding zeker stelt, ten aanzien van de gegevensverwerking voor netwerkplanning en -beheer in deze specifieke context via de door KPN voorgestelde anonimiseringsoplossing geen overtreding van artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

De (mogelijke) toekomstige inzet van data-analyse technieken voor de behandeling van klantklachten via een nieuw(e), gescheiden systeem/[VERTROUWELIJK: apparatuur]-omgeving valt buiten de scope van dit onderzoek.

⁴³¹ Zie o.a. reactie KPN op vordering van 28 februari 2013, p. 1.