COLLEGE BESCHERMING PERSOONSGEGEVENS

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

College bescherming persoonsgegevens

Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door T-Mobile Netherlands B.V.

Z2011-00462

Rapport definitieve bevindingen

Mei 2013 met erratum van 11 juni 2013

OPENBARE VERSIE

Inhoudsopgave

Bijlagen:

I. Overzicht mobiel netwerk
II. Overzicht verwerkte gegevens, per doeleinde
III. Verklarende woordenlijst
IV. Zienswijze 1 T-Mobile, met de reactie daarop van het CBP
V. Zienswijze 2 T-Mobile, met de reactie daarop van het CBP

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar de wijze waarop T-Mobile *packet inspection* technologie en technieken (hierna: data-analysetechnieken) toepast in het mobiele netwerk van het bedrijf. Onder data-analysetechnieken wordt verstaan: technieken waarmee gegevens over en uit het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd. Het CBP heeft onderzocht of T-Mobile hierbij persoonsgegevens verwerkt en zo ja, of T-Mobile 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-analysetechnieken - 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 T-Mobile

T-Mobile verwerkt gegevens over en uit het dataverkeer van circa 2,8 miljoen T-Mobile 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.

T-Mobile verwerkt de persoonsgegevens voor de volgende onderzochte doeleinden

- netwerkbeheer en -integriteit (waaronder netwerkplanning en -beheer, virus- en malwarebestrijding en het oplossen en voorkomen van netwerkproblemen)
- troubleshooting (het oplossen van technische incidenten en klantproblemen in individuele gevallen)
- optimalisatie van de dienstverlening aan klanten (videocompressie).

T-Mobile inspecteert en analyseert 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 T-Mobile ook op inhoud teneinde virussen en malware tegen te houden en te verwijderen.

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Één daarvan is bijvoorbeeld dat er altijd een wettelijke rechtvaardigingsgrond (grondslag) voor de gegevensverwerking moet bestaan. Het CBP heeft bij T-Mobile gedurende het

onderzoek een aantal overtredingen van de Wbp én de Tw geconstateerd, die inmiddels gedeeltelijk zijn beëindigd.

Overtredingen die nog niet zijn beëindigd

Netwerkbeheer en -integriteit
Het verwerken van persoonsgegevens voor netwerkbeheer is alleen toegestaan als de persoonsgegevens zo snel mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren.

T-Mobile verwijdert voor netwerkplanning en -beheer wat betreft één specifieke gegevensverwerking met betrekking tot websitebezoek of app- en protocolgebruik het verzamelde 06-nummer zo snel mogelijk. Omdat T-Mobile eventuele e-mailadressen niet zo snel mogelijk verwijdert, is het bedrijf op dat punt toch in overtreding.

Omdat T-Mobile voor netwerkplanning en -beheer wat betreft een andere gegevensverwerking met betrekking tot hooggebruik van data het verzamelde 06-nummer niet zo snel mogelijk verwijdert, is het bedrijf in overtreding.

Overtredingen die gedeeltelijk zijn beëindigd

Informeren abonnees
T-Mobile 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. T-Mobile informeerde abonnees bij aanvang van het onderzoek niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking bij de toepassing van data-analysetechnieken. Daarnaast informeerde T-Mobile hen niet over de categorieën van verwerkte persoonsgegevens en de bewaartermijnen. T-Mobile was hierdoor in overtreding.

T-Mobile heeft de privacyverklaring van het bedrijf aangepast, voor het laatst in december 2012. Door deze getroffen maatregel zijn de geconstateerde overtredingen gedeeltelijk beëindigd. Er ontbreekt echter nog informatie over de bewaartermijnen.

Overtredingen die zijn beëindigd

Netwerkbeheer en -integriteit
Omdat T-Mobile voor het oplossen en voorkomen van netwerkproblemen bij aanvang van het onderzoek de verzamelde persoonsgegevens niet zo snel mogelijk verwijderde, was het bedrijf in overtreding.

Naar aanleiding van het onderzoek heeft T-Mobile de bewaartermijnen van de persoonsgegevens voor het oplossen en voorkomen van netwerkproblemen aanzienlijk verkort. Door deze getroffen maatregel zijn de geconstateerde overtredingen op dit punt beëindigd.

Meldingsplicht
Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen wettelijk verplicht deze gegevensverwerking te melden bij het CBP. De meldingen van T-

Mobile waren bij aanvang van het onderzoek niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking. T-Mobile was hierdoor in overtreding.

T-Mobile heeft de meldingen bij het CBP inmiddels gewijzigd. Door deze getroffen maatregel zijn de geconstateerde overtredingen op dit punt beëindigd.

Geen overtredingen geconstateerd

Virus- en malwarebestrijding, troubleshooting en videocompressie
T-Mobile heeft een wettelijke grondslag voor de verwerking ten behoeve van virus- en malwarebestrijding, troubleshooting en videcompressie. Op deze punten is T-Mobile dan ook niet in overtreding (geweest).

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 T-Mobile Netherlands B.V. (hierna: T-Mobile) in haar mobiele netwerk *packet inspection* technologie en technieken (hierna: data-analysetechnieken) toepast.

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

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

Achtergrond onderzoek

Een belangrijke reden voor veel mobiele netwerkaanbieders 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.

Aanleiding onderzoek

Mobiele netwerken bestaan vandaag de dag vaak uit een of meer GSM-gedeeltes (voor de afhandeling van spraakverkeer) en GPRS/UMTS-gedeeltes (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.

Smartphones verbreken veelvuldig de verbinding om de batterij te sparen. Er zijn applicaties (*apps)* die vaak weer verbinding (doen) zoeken met het netwerk, om gegevens te verversen door data van de server af te halen of te checken of er updates beschikbaar zijn. 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- of UMTS-gedeelte kan er ook niet meer worden gebeld.

---

[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 (soorten) 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 datasessie etc.

Een belangrijke reden voor veel telecombedrijven om data-analysetechnieken in te zetten is netwerkbeheer, om problemen in het netwerk te detecteren en op te lossen en om de gevolgen van congestie te beperken.[3]

Data-analysetechnieken worden in de huidige praktijk - naast een breed scala andere technieken - 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, behandeling van klantklachten en marktonderzoek.

Het gebruik van data-analysetechnieken raakt in potentie veel mensen. Volgens gegevens uit de jaarlijkse marktmonitor van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: OPTA, per 1 april 2013 de Autoriteit Consument en Markt, hierna: ACM) waren er aan het einde van het derde kwartaal van 2011 in totaal 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

[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: 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', *Nieuwsbericht OPTA* 23 april 2012. URL: https://www.acm.nl/nl/publicaties/publicatie/10347/OPTA-jaarverslag-en-marktmonitor-2011/. Presentatie marktmonitor 2011, *Presentatie OPTA* 23 april 2012. URL: https://www.acm.nl/nl/publicaties/publicatie/10346/Presentatie-marktmonitor-2011/ (URL's 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."* 'Telecommonitor 2012: Lagere omzet voor mobiele aanbieders door minder sms'jes', *Nieuwsbericht* OPTA 17 april 2013. URL: https://www.acm.nl/nl/publicaties/publicatie/11338/Telecommonitor-2012-Lagere-omzet-voor-mobiele-aanbieders-door-minder-smsjes/. Zie ook Openbare rapportage mobiel Q4 2012, p. 1. URL: https://www.acm.nl/nl/download/bijlage/?id=10942 (URL's 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 1.185.000 specifieke mobiele breedbandinternet aansluitingen, zoals tablets en dongels. In totaal 10.248.000 mobiele internetaansluitingen, ofwel 46,4 procent van het totaal aantal mobiele aansluitingen. Tabel "Mobiel: Aantal retailaansluitingen" uit de Openbare rapportage mobiel Q4 2012, p. 1. Het feitelijke percentage smartphone abonnees met internettoegang verschilt per mobiele aanbieder. 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. Vgl. ook 'Marktrapportage elektronische communicatie (MEC) eerste helft 2012 is uit', *TNO* 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's laatst bezocht op 29 mei 2013). Op basis van het aantal aansluitingen voor mobiele telefonie ligt het marktaandeel van T-Mobile volgens de Openbare rapportage mobiel Q4 2012 aan het eind van 2012 tussen 20 en 25 procent. Openbare rapportage mobiel Q4 2012, p. 2.

van bijna 2,5% van de mobiele telefonieaansluitingen met een data abonnement.[7]

OPTA heeft in mei en juni 2011 onderzoek (een *quick scan*) 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 geconcludeerd dat er in dat stadium op basis van de Tw geen aanleiding was voor handhavend optreden.[8] OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van het Samenwerkingsprotocol CBP-OPTA van 12 juli 2005 (hierna: Samenwerkingsprotocol CBP-OPTA).[9]

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.[10]

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."*[11]

---

[7] Aan het eind van het eerste kwartaal van 2013 had Tele2 535.000 mobiele abonnees. Omgerekend vanuit het gegeven dat gemiddeld 46,4% van de mobiele abonnees in Nederland ook een data abonnement heeft, bedient Tele2 bijna 250.000 abonnees met internettoegang. Dit resulteert in een marktaandeel van 2,4 procent. URL: http://reports.tele2.com/2013/Q1/index.html (URL laatst bezocht op 29 mei 2013).

[8] 'Voorlopige bevindingen over gebruik Deep Packet Inspection Voorlopige bevindingen over gebruik Deep Packet Inspection', *Onderzoek OPTA* 30 juni 2011. URL: https://www.acm.nl/nl/publicaties/publicatie/10234/Voorlopige-bevindingen-over-gebruik-Deep-Packet-Inspection/ (URL laatst bezocht op 29 mei 2013).

[9] *Stcrt.* 2005, 133.

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

[11] *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*

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 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), voor zover voor dit onderzoek van belang, 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).[12] 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 T-Mobile verzamelt en verwerkt persoonsgegevens, zoals gedefinieerd in artikel 1, aanhef en onder a, van de Wbp?
- Zijn de doeleinden waarvoor T-Mobile 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 T-Mobile als bedoeld in artikel 8 van de Wbp?
- Heeft T-Mobile de betrokkenen (tijdig) geïnformeerd over de gegevensverwerking, zoals bepaald in artikel 34 van de Wbp?
- Heeft T-Mobile 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?

---

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* [behoudens het bepaalde in artikel 15.1, eerste lid, onder h, van de Tw, toevoeging door het CBP]. *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.

[12] Zie artikel 2 van het Besluit aanwijzing toezichthouders Telecommunicatiewet. Artikel 1, derde lid, van de Samenwerkingsovereenkomst Agentschap Telecom-College bescherming persoonsgegevens van 15 september 2009 (hierna: Samenwerkingsovereenkomst Agentschap Telecom-CBP) 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. *Stcrt.* 2009, 13672.

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.[13]

OPTA heeft op 30 juni 2011 haar voorlopige bevindingen gepubliceerd.[14]

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) op grond van artikel 10, eerste en derde lid, van het Samenwerkingsprotocol CBP-OPTA 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 T-Mobile. T-Mobile heeft het CBP bij brief van 1 september 2011 verzocht om uitstel van de termijn voor het geven van een reactie tot en met 8 september 2011. Het CBP heeft T-Mobile bij brief van 1 september 2011 het gevraagde uitstel verleend. T-Mobile heeft de inlichtingen (grotendeels) bij brief van 8 september 2011 (door het CBP ontvangen op 12 september 2011) aan het CBP verstrekt.

Bij brief van 13 september 2011 heeft het CBP T-Mobile verzocht het ontbrekende antwoord op het inlichtingenverzoek van 18 augustus 2011 uiterlijk op 19 september 2011 alsnog aan het CBP te verstrekken. T-Mobile heeft het ontbrekende antwoord op 19 september 2011 aan het CBP verstrekt.

Bij brief van 11 oktober 2011 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij T-Mobile. T-Mobile heeft bij brief van 13 oktober 2011 verzocht om uitstel van de termijn voor het geven van een reactie tot en met 25 oktober 2011. Het CBP heeft bij brief van 13 oktober 2011 uitstel verleend tot en met 24 oktober 2011. T-Mobile heeft de gevraagde inlichtingen op 24 oktober 2011 aan het CBP verstrekt.

Het CBP heeft T-Mobile bij brief van 11 oktober 2011 aangekondigd een onderzoek ter plaatse te zullen uitvoeren bij T-Mobile. Op 17 oktober 2011 heeft het onderzoek ter plaatse plaatsgevonden ten kantore van T-Mobile in Den Haag. Tijdens genoemd onderzoek hebben medewerkers van het CBP mondeling inlichtingen ingewonnen bij de [VERTROUWELIJK], de [VERTROUWELIJK] en [VERTROUWELIJK][15] van T-Mobile alsmede een aantal (kopieën van) bescheiden gevraagd. Daarnaast heeft het

[13] 'Voorlopige bevindingen OPTA over gebruik Deep Packet Inspection', *Nieuwsbericht 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).
[14] 'Voorlopige bevindingen over gebruik Deep Packet Inspection', *Onderzoek OPTA* 30 juni 2011.
[15] Allen gevolmachtigd om tijdens dit onderzoek ter plaatse namens T-Mobile het woord te voeren.

CBP gebruikersinterfaces bekeken van de apparatuur die T-Mobile inzet voor data-analyse.

Het CBP heeft een aantal (kopieën van) bescheiden meegenomen, in de vorm van een USB-stick van 8 GB, de schriftelijke volmacht en 8 print-outs (screenshots) van 1 A4.[16] T-Mobile heeft de overige gevraagde antwoorden en (kopieën van) bescheiden (zoals genoemd in een brief van het CBP van 17 oktober 2011) op 19 respectievelijk 24 oktober 2011 aan het CBP verstrekt.

Op 25 november 2011 heeft het CBP mondeling een stuk bij T-Mobile opgevraagd. T-Mobile heeft dit stuk bij e-mail van 28 november 2011 aan het CBP verstrekt.

Op 1 december 2011 heeft het CBP mondeling inlichtingen ingewonnen bij T-Mobile.

Op 9 december 2011 heeft het CBP mondeling (bevestigd per e-mail) inlichtingen ingewonnen bij T-Mobile. T-Mobile heeft de gevraagde inlichtingen op 15 december 2011 schriftelijk aan het CBP verstrekt.

Het CBP heeft op 12 januari 2012 het rapport voorlopige bevindingen vastgesteld. Het CBP heeft T-Mobile bij brief van 13 januari 2012 in de gelegenheid gesteld om haar zienswijze op het rapport voorlopige bevindingen naar voren te brengen. T-Mobile heeft bij brief van 6 februari 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 2 maart 2012. Het CBP heeft bij brief van 9 februari 2012 uitstel verleend tot en met 24 februari 2012. T-Mobile heeft haar zienswijze op 24 februari 2012, aangevuld op 5 maart 2012, schriftelijk ingebracht.

Op 10 februari 2012 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en [VERTROUWELIJK] van T-Mobile over het onderzoek (bevestigd per e-mail).

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

Op 11 juni 2012 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en de [VERTROUWELIJK] van T-Mobile over het onderzoek.

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 Agentschap Telecom respectievelijk OPTA.

Op 17 juli 2012 heeft het CBP mondeling twee stukken bij T-Mobile opgevraagd. T-Mobile heeft deze stukken bij e-mail van 17 juli 2012 aan het CBP verstrekt.

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

[16] Van de tijdens het onderzoek ter plaatse opgestelde en geprinte/gekopieerde bescheiden is een kopie aan T-Mobile verstrekt.

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 T-Mobile bij brief van 21 augustus 2012 in de gelegenheid gesteld om haar zienswijze op het Conceptrapport definitieve bevindingen naar voren te brengen. T-Mobile heeft bij brief van 25 september 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 30 oktober 2012. Het CBP heeft bij brief van 25 september 2012 het door T-Mobile gevraagde uitstel verleend. T-Mobile heeft haar zienswijze op 30 oktober 2012 schriftelijk ingebracht.

Bij brief van 12 december 2012 heeft het CBP T-Mobile bericht over de voortgang van het onderzoek.

Op 20 december 2012 heeft het CBP een vordering om inlichtingen en inzage in zakelijke gegevens en bescheiden aan T-Mobile gezonden.

T-Mobile heeft het CBP bij e-mail van 21 december 2012 geïnformeerd over de wijziging van haar Privacy Statement per 10 december 2012 en de wijziging van haar melding met nummer m1070731 per 30 oktober 2012.

T-Mobile heeft bij brief van 4 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 21 februari 2013. Het CBP heeft bij brief van 9 januari 2013 het door T-Mobile gevraagde uitstel verleend.

T-Mobile heeft bij brief van 21 februari 2013 gereageerd op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden.

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 Agentschap Telecom.

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

Zienswijze 1 van T-Mobile van 24 februari 2012 op het Rapport voorlopige bevindingen

In haar zienswijze van 24 feburari 2012 op het Rapport voorlopige bevindingen (hierna: zienswijze 1) brengt T-Mobile, samengevat weergegeven, naar voren dat het rapport voorlopige bevindingen onzorgvuldig is voorbereid en ontoereikend is gemotiveerd.

Het CBP moet in zijn beoordeling volgens T-Mobile uitgaan van de feitelijk bij T-Mobile bestaande situatie, zoals die door T-Mobile aan het CBP is uiteengezet.

T-Mobile betwist dat er bij de huidige stand van zaken technische alternatieven voor data-analyse zijn.

T-Mobile geeft aan dat de gegevens die T-Mobile verwerkt door middel van toepassing van data-analysetechnieken niet de inhoud van communicatie (*payload*) betreft, maar internetverkeersgegevens.

T-Mobile betoogt dat de gegevensverwerkingen worden geregeerd door de Tw en de roamingverordening die gelden als lex specialis ten opzichte van de Wbp.

De doeleinden waarvoor T-Mobile deze gegevens verwerkt, vallen volgens T-Mobile binnen de wettelijke grondslagen in de Tw en de roamingverordening.

Voor zover er sprake is van de verwerking van persoonsgegevens kunnen daaraan volgens T-Mobile de volgende grondslagen ten grondslag worden gelegd: uitvoering van een overeenkomst met haar abonnees, nakoming van wettelijke verplichtingen en ter behartiging van een gerechtvaardigd belang van T-Mobile, waarbij er geen sprake van is dat de belangen van haar abonnees of de gebruikers van haar dataverkeersdiensten onevenredig worden aangetast (artikel 8, aanhef en onder b, c en f, van de Wbp).

T-Mobile betwist dat alle door T-Mobile verwerkte gegevens moeten worden aangemerkt als persoonsgegevens: T-Mobile geeft aan dat veel van haar abonnees ondernemingen en/of rechtspersonen zijn en dat zij ook waar het gaat om de internetdienstverlening in treinen geen kennis heeft van de identiteit van de gebruikers van haar dataverkeersdiensten, zodat geen sprake kan zijn van persoonsgegevens.

T-Mobile betwist dat zij haar abonnees en de gebruikers van haar dataverkeersdiensten niet voldoende heeft geïnformeerd over de gegevensverwerkingen en dat zij zich niet heeft gehouden aan de meldplicht bij het CBP.

T-Mobile geeft aan dat zij, zonder aanvaarding van enige gehoudenheid daartoe, aanleiding heeft gezien om haar privacy statement en de meldingen bij het CBP aan te passen.

In **bijlage IV** bij dit rapport is de zakelijke inhoud van de zienswijze 1 van T-Mobile opgenomen per onderdeel (met de toevoeging '**Zienswijze 1 T-Mobile**'), met de reactie daarop van het CBP (zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd en aangevuld met in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van dat Conceptrapport definitieve bevindingen). Deze bijlage vormt een integraal onderdeel van dit rapport.

Zienswijze 2 van T-Mobile van 30 oktober 2012 op het Conceptrapport definitieve bevindingen

In haar zienswijze 2 van 30 oktober 2012 op het Conceptrappor definitieve bevindingen (daaronder in dit geval mede begrepen de daaropvolgende correspondentie als beschreven onder het kopje 'Verloop onderzoek', p. 9 e.v. van dit rapport) brengt T-Mobile, samengevat weergegeven, naar voren dat de reikwijdte van het onderzoek verschillende keren en op een voor T-Mobile niet inzichtelijke wijze is

veranderd en opgerekt of verbreed. De verandering en oprekking of verbreding van de onderzoeksdoeleinden duiden volgens T-Mobile op een *fishing expedition* en staan als zodanig op gespannen voet met zorgvuldigheidsvereisten, het verbod van willekeur en het verdedigingsbeginsel.

T-Mobile meent dat het feitenonderzoek door het CBP ontoereikend is en dat het rapport ook in verschillende andere opzichten niet voldoet aan daaraan te stellen zorgvuldigheids- en andere vereisten (het verbod van willekeur en het verdedigingsbeginsel). Zo heeft het CBP volgens T-Mobile onvoldoende onderzocht, althans niet deugdelijk gemotiveerd dat er andere mogelijkheden of andere manieren zijn om hetzelfde doel te bereiken zijn én of deze oplossingen zonder onoverkomelijke risico's in het mobiele netwerk van T-Mobile kunnen worden geïmplementeerd, evenals de kosten van dergelijke oplossingen, de implicaties daarvan in termen van de betrouwbaarheid van de dienstverlening, de operationele gevolgen ervan, de eindgebruikerservaring etc.

T-Mobile stelt zich op het standpunt dat het CBP niet een Rapport definitieve bevindingen kan vaststellen, maar haar (eerst) opnieuw gelegenheid dient te bieden tot het geven van zienswijzen.

Volgens T-Mobile blijkt uit het Conceptrapport definitieve bevindingen of het CBP is uitgegaan van de feitelijke instellingen van de gebruikte data-analyse apparatuur.

Volgens T-Mobile verlangt het CBP van haar dat zij bewijst onschuldig te zijn.

T-Mobile heeft nut en noodzaak van data-analyse in mobiele netwerken nader toegelicht.[17]

T-Mobile maakt bezwaar tegen (de vorm van) de bronvermeldingen.

T-Mobile merkt op dat in het Rapport voorlopige bevindingen werd verwezen naar documenten waarvan de inhoud voor T-Mobile onbekend is.

T-Mobile meent dat het Conceptrapport definitieve bevindingen suggestieve en tendentieuze opmerkingen en verdachtmakingen bevat, die moeten worden verwijderd.

T-Mobile meent dat bij geen van de in het rapport beoordeelde gegevensverwerkingen sprake is of was van overtredingen van de Wbp en/of Tw (zij verwijst daarbij ook naar haar zienswijze 1).

Volgens T-Mobile is het Conceptrapport definitieve bevindingen niet eenduidig over wat volgens het CBP als overtreding moet worden gekwalificeerd.

T-Mobile meent dat waar het gaat om de gestelde overtreding met betrekking tot de verwerkingsgrondslag de structuur van het rapport onduidelijk is en de argumentatie moeilijk te volgen, vooral doordat feitelijke, opiniërende en normatieve beschrijvingen door elkaar lopen. Verder lijkt volgens T-Mobile sprake van een *one-size-fits-all*

[17] Zie ook reactie T-Mobile op vordering van 21 februari 2013, p. 7.

benadering die geen recht doet aan de concrete en specifieke omstandigheden van T-Mobile, in strijd met het zorgvuldigheids-, verdedigings-, en lex certa-beginsel (rechtszekerheidsbeginsel), alsmede het verbod van willekeur en de onschuldpresumptie.

T-Mobile geeft aan dat zij de privacyverklaring van het bedrijf heeft aangepast en de meldingen bij het CBP heeft gewijzigd.[18]

T-Mobile heeft de bewaartermijnen van de persoonsgegevens voor het oplossen en voorkomen van netwerkproblemen verkort.

In **bijlage V** bij dit rapport is de zakelijke inhoud van de zienswijze 2 van T-Mobile opgenomen per onderdeel (met de toevoeging '**Zienswijze 2 T-Mobile**'), met de reactie daarop van het CBP en in hoeverre 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.

[18] E-mail T-Mobile van 21 december 2012.

2. Feitelijke Bevindingen

2.1 Organisatiebeschrijving

T-Mobile, gevestigd te Den Haag, is ingeschreven bij de Kamer van Koophandel sinds 5 juli 1984, onder nummer 33265679. De doelomschrijving van T-Mobile is: *"Holdingmaatschappij; Het exploiteren, het aanvragen van en, indien mogelijk, het verkrijgen van licenties voor het installeren, onderhouden en functioneren van een vaste telecommunicatie infrastructuur en een mobiele telecommunicatie infrastructuur in Nederland; Het (doen) verlenen van toegang tot internet, verstrekken van informatie ten behoeve van derden met betrekking tot mogelijkheden om op internet mededelingen/publicatie te doen, ontwikkelen en verkopen van software (groothandel), verstrekken van wereldwijde netservice voor internet en de automatisering."*

T-Mobile is geregistreerd bij de ACM als aanbieder van een openbare elektronische communicatiedienst en -netwerk.[19]

T-Mobile verklaarde in 2011 4,5 miljoen abonnees te hebben als aanbieder van mobiele aansluitingen in Nederland, en per eind 2012 4,7 miljoen.[20] Omgerekend levert dat een marktaandeel op de markt voor mobiele telefonie in Nederland op van 20-25%.[21] Niet alle T-Mobile-klanten hebben ook toegang tot mobiel internet. Uit de Openbare rapportage mobiel Q4 2012 blijkt dat ongeveer 46,4% van de Nederlandse mobiele telefonieaansluitingen eind 2012 toegang had tot mobiel internet.[22] Volgens recente gegevens van Telecompaper heeft meer dan 60% van de T-Mobile abonnees in Nederland inmiddels mobiel internet.[23] Omgerekend voor T-Mobile betreft het bijna 2,8 miljoen abonnees.

---

[19] URL: https://www.acm.nl/nl/onderwerpen/telecommunicatie/registraties/geregistreerde-ondernemingen/resultaat/?query=T-Mobile&categorie=&plaats= (URL laatst bezocht op 29 mei 2013).

[20] Zie o.a. reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 1 en reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 1. Op de website van T-Mobile staat vermeld: *"Klanten 4,7 miljoen (per 31 december 2012)."* URL: http://www.t-mobile.nl/corporate/htdocs/page/over-t-mobile/t-mobile.aspx. Volgens gegevens uit de halfjaarlijkse Marktrapportage Elektronische Communicatie van TNO had T-Mobile aan het einde van het tweede kwartaal van 2011 4,8 miljoen mobiele aansluitingen. TNO-rapport. 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 (URL's laatst bezocht op 29 mei 2013).

[21] 'Openbare rapportage mobiel Q4 2011 van OPTA', *Onderzoek OPTA* 1 mei 2012. URL: http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3584. Volgens gegevens uit de halfjaarlijkse Marktrapportage Elektronische Communicatie van TNO steeg het marktaandeel mobiele telefonieaansluitingen van T-Mobile in 2011 naar 24,2%. TNO-rapport. Marktrapportage Elektronische Communicatie December 2011, Delft: TNO 2011, p. 15. Zie ook OPTA jaarverslag 2012, p. 10. URL: http://optajaarverslag2012.acm.nl (URL's laatst bezocht op 29 mei 2013). Openbare rapportage mobiel Q4 2012, p. 2.

[22] Openbare rapportage mobiel Q4 2012, p. 1. Zie ook OPTA jaarverslag 2012, p. 7: *"Ruim 45 procent van de aansluitingen voor mobiele telefoons wordt ook gebruikt voor internet."*

[23] 'Consumenten kopen handset in winkel, bestellen sim online', *Telecompaper* 11 juli 2012.

Van het totaal aantal T-Mobile mobiele telefonie abonnees met mobiel internet hebben er volgens cijfers van T-Mobile [VERTROUWELIJK] een prepaid aansluiting [VERTROUWELIJK]. T-Mobile schrijft: *"Alle T-Mobile prepaid klanten hebben de mogelijkheid om gebruik te maken van mobiel internet. Het is echter afhankelijk van het type toestel of daadwerkelijk toegang tot mobiel internet kan worden verkregen. Het aantal T-Mobile prepaid aansluitingen is dan ook niet gelijk aan het aantal prepaid klanten die gebruik kunnen maken van mobiel internet."*[24] Van de hierboven genoemde [VERTROUWELIJK] prepaid abonnees maken er volgens cijfers van T-Mobile gemiddeld [VERTROUWELIJK] weleens gebruik van mobiele data diensten [VERTROUWELIJK]. T-Mobile heeft NAW-gegevens en/of e-mailadressen van [VERTROUWELIJK] van het totaal aantal prepaid abonnees.[25] [VERTROUWELIJK]

T-Mobile heeft de verwerking van persoonsgegevens, voor zover voor dit onderzoek van belang, op 22 februari 2010 (gewijzigd) gemeld bij het CBP onder nummers m1070731 en m1070767 (versienummers 5.0). In de meldingen zijn, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

'Accounts Records Management Systeem' (m1070731)

Het registreren van gegevens over afgewikkeld verkeer van spraak en data ten behoeve van onderzoek naar hoogverbruik en (intern) fraudeonderzoek.[26]

'Klantmanagement- en billingsysteem' (m1070767)

Het sluiten en uitvoeren van de overeenkomst die het gevolg is van een aansluiting.
Het analyseren van het gebruik van het netwerk.
Het nakomen van wettelijke verplichtingen.[27]

T-Mobile heeft verklaard dat de meldingen met nummers m1070731 en m1070767 geen betrekking hebben op de inzet van data-analysetechnieken in haar mobiele netwerk: "*Ten aanzien van de doeleinden zoals beschreven in de (…)*

[24] Reactie T-Mobile op verzoek om inlichtingen van 11 april 2012, p. 1.
[25] T-Mobile verkrijgt NAW-gegevens en/of e-mailadressen van prepaid abonnees (i) via een My T-Mobile account op de T-Mobile website, een persoonlijke online omgeving met abonneegegevens, factuur- dan wel beltegoedinformatie, en instellingen (registratie van MSISDN (06-nummer) en e-mailadres is verplicht bij het aanmaken van een account), (ii) via het spaarprogramma 'T-Mobile speciaal' (als een prepaid abonnee zijn NAW-gegevens registreert, krijgt hij daarvoor spaarpunten die kunnen worden ingewisseld voor beltegoed), (iii) indien een postpaid abonnee prepaid klant wordt met behoud van zijn telefoonnummer, (iv) in het geval een prepaid abonnee belt naar de klantenservice met een nummer gerelateerde vraag, zoals 'Ik ben mijn pin/puk code kwijt, kunt u mij deze alsnog geven?' en (v) via de online game voor prepaid abonnees 'T-Mobile Surprise' (daarmee kunnen prijzen worden gewonnen, indien de prepaid abonnee een prijs wint dient hij zijn NAW-gegevens door te geven voor de adressering/verzending). Reactie T-Mobile op verzoek om inlichtingen van 11 april 2012, p. 1-2.
[26] In de melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens genoemd: 'klanten van T-Mobile' respectievelijk 'NAW-gegevens', 'IMSI nummer' (uniek klantnummer), 'Nummer oproeper / opgeroepene' (MSISDN), 'tijd/datum/duur/soort gesprek', 'gesprekslocatie' (zendmastgegevens), 'IMEI-nummer' (uniek toestelnummer), 'billing data' en 'individuele tariefvoorwaarden'.
[27] In de melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens genoemd: 'klanten' respectievelijk 'NAW-gegevens', 'afgenomen producten / diensten', 'gespreksgegevens', 'rekeninginformatie' en 'telefoon- en faxnummer'.

bovengenoemde meldingen kan T-Mobile bevestigen dat er geen sprake is van het analyseren van mobiele datapakketten in het T-Mobile netwerk. De meldingen betreffen gegevensverwerkingen van data welke verkregen is in het kader van de uitvoering van de dienst dan wel de overeenkomst. Zoals reeds in de meldingen wordt aangegeven hebben de gegevensverwerkingen tot doel

1. *het tijdig signaleren van hoogverbruik (en daarmee het voorkomen van de zogenaamde 'bill shock' bij de klant) op grond van voice/data volumes (m1070731);*
2. *het beheren van de klant relatie dan wel het kunnen opstellen van de factuur op grond van door de klant verstrekte gegevens en Call Detail Records welke gegenereerd worden in het netwerk (m1070767) (…)."*[28]

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

Getroffen maatregelen

T-Mobile heeft de meldingen met nummers m1070731 en m1070767 op 23 december 2011 gewijzigd (versienummers 6.0).

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

'Netwerkbeheer en gebruikersmanagement' (m1070731)

Analyseren van gebruik van het netwerk, onder andere aan de hand van afgewikkeld verkeer van spraak en data.
Het bevorderen van de beveiliging en integriteit van het netwerk en de diensten van verantwoordelijke en het waarborgen van de continuïteit en de belangen van verantwoordelijke(n), waaronder verkeersbeheer, (individuele) troubleshooting en het voorkomen van fraude, misbruik en hooggebruik.
Uitvoering of toepassing van relevante wet- en regelgeving (inclusief bewaarplicht telecommunicatiegegevens en telefonisch overlast).[29]

'Klantmanagement- en facturering' (m1070767)

Het beoordelen van de aanvraag van de afname van diensten en producten van verantwoordelijke en het sluiten en uitvoeren van de overeenkomst, waaronder facturering.
Het bevorderen van de beveiliging en integriteit van de diensten van verantwoordelijke en het waarborgen van de continuïteit en de belangen van verantwoordelijke, waaronder verkeersbeheer en het voorkomen van fraude, misbruik en hooggebruik.
Marktonderzoek, verkoopactiviteiten, kwaliteitsmonitoring en opleiding van medewerkers van verantwoordelijke en/of derden.

[28] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 6.
[29] In de gewijzigde melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens genoemd: 'gebruikers van de diensten en producten van T-Mobile' respectievelijk 'telefoonnummer' (MSISDN), 'IMSI/IMEI nummer' (uniek klant- en toestelnummer), 'accountgegevens, inclusief gebruikersnaam en e-mailadres', 'verkeersgegevens', 'andere identifiers ten behoeve van het tot stand brengen van de communicatie, en het leveren van gevraagde diensten' en 'locatiegegevens'.

Uitvoering of toepassing van relevante wet- en regelgeving (inclusief bewaarplicht telecommunicatiegegevens en telefonische overlast).[30]

T-Mobile heeft de melding met nummer m1070731 op 30 oktober 2012 opnieuw gewijzigd (versienummers 8.0). In de gewijzigde meldingen is, voor zover voor dit onderzoek van belang, als doel van verwerking toegevoegd:

'Netwerkbeheer en gebruikersmanagement' (m1070731)

Optimaliseren van de dienstverlening aan haar gebruikers {waaronder begrepen videocompressie}

2.2 Mobiel netwerk, netwerkverkeer, plaatsing data-analyse apparatuur en opbouw datapakketten

Het mobiele netwerk van T-Mobile 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 T-Mobile 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 tot het radiotoegangsnetwerk). Elk onderdeel van het mobiele netwerk heeft een maximum capaciteit (zie ook het kopje 'Aanleiding onderzoek', p. 5 e.v. van dit rapport).

Het GPRS/UMTS-gedeelte van het mobiele radiotoegangsnetwerk bestaat uit *Base Stations* (*'Node B';* antenne radiomast) en *Radio Network Controllers* (RNC; netwerkelement waar de gegevens worden versleuteld voordat deze worden verzonden naar en van het mobiele apparaat). In het core-netwerk bevinden zich databases[31] en netwerkelementen die nodig zijn voor het leveren van diensten, zoals *Serving GPRS Support Nodes* (SGSN) die de binnenkomende radiosignalen omzetten in GTP-*controle plane* (GTP-C; oftewel, het signaleringskanaal) en GTP-*user plane* (GTP-U; oftewel, het dataverkeer kanaal) en de *Gateway GPRS Support Nodes* (GGSN) die het dataverkeer doorgeven aan externe netwerken, zoals het internet.

[30] In de gewijzigde melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens genoemd: 'Toekomstige klanten', 'Klanten' en 'Voormalige klanten' respectievelijk 'naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode', 'woonplaats, telefoonnummer, e-mailadressen', 'soortgelijke voor communicatie benodigde gegevens', 'gegevens over het gebruik van de afgenomen diensten en producten (inclusief servicegegevens, abonnementsgegevens en verkeersgegevens)' en 'logbestanden van klantenservice en customer sales'.

[31] Bijvoorbeeld het *Home Location Register* (databank waarin onder meer het MSISDN, het IMSI en informatie over de (prepaid of postpaid) datadiensten waar de abonnee op is geabonneerd, zijn opgeslagen) en het *Visitor Location Register* (databank waarin de exacte locatie van gebruikers van het mobiele netwerk wordt bijgehouden).

T-Mobile maakt gebruik van data-analysetechnieken op het dataverkeer (inclusief signaleringsverkeer) in haar mobiele netwerk.[32] Daartoe zijn op verschillende punten in het netwerk verschillende soorten data-analyse apparatuur geplaatst, [VERTROUWELIJK] (zie **bijlage I**).

Met gebruikmaking van de data-analyse apparatuur inspecteert en analyseert T-Mobile, kort gezegd, datapakketten/datapakketgegevens. Daartoe worden datapakketten door/langs een filter met inspectieregels geleid. Data-analyse apparaten verwerken niet meer dan dat waarvoor ze zijn ingesteld. T-Mobile heeft een aantal apparaten, en zij doet niet met elk apparaat hetzelfde.

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').

T-Mobile verkrijgt via de data-analyse apparatuur[33] gegevens over en (in een enkel geval) uit het dataverkeer van potentieel alle[34] ongeveer 2,8 miljoen T-Mobile abonnees met een (prepaid of postpaid) data abonnement en van de gebruikers van haar dataverkeersdiensten.

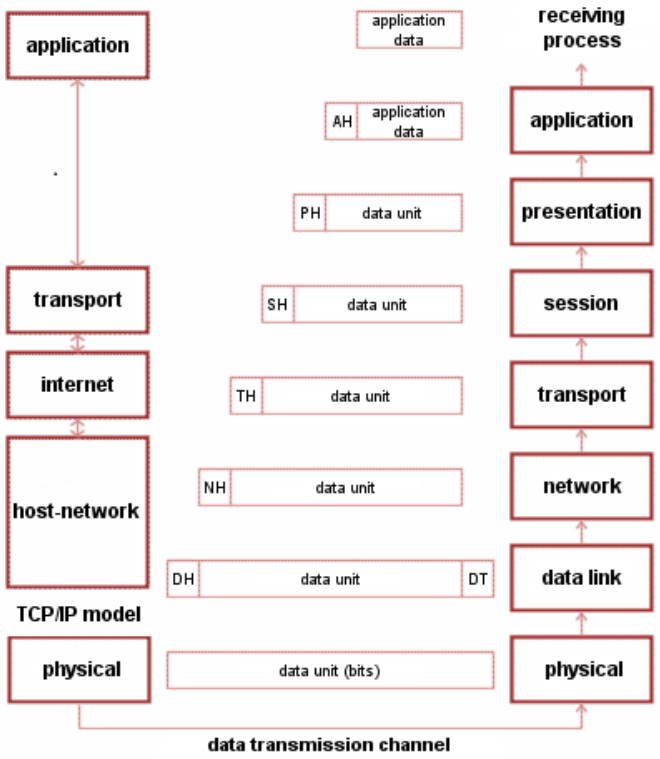
De gegevens 'over' en 'uit' het dataverkeer (inclusief signaleringsverkeer) worden hier, ter illustratie, beschreven aan de hand van de verschillende lagen van het ISO-OSI-model (hierna: OSI-model) en het TCP-IP model. Beide modellen zijn een gestandaardiseerde indeling van netwerkverkeer in respectievelijk 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.

[32] Zie o.a. reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2 en bijlage 1 bij deze reactie over de plaatsing van de data-analyse apparatuur in het netwerk; reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1 en bijlage 2 bij deze reactie over de plaatsing van de data-analyse apparatuur in het netwerk. Vgl. ook reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2012 met kenmerk [VERTROUWELIJK], p. 2: [VERTROUWELIJK].

[33] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3; reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, bijlage 1 en e-mail T-Mobile van 15 december 2011.

[34] Vgl. reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 5: [VERTROUWELIJK].

AFBEELDING 1 Opbouw packets volgens TCP-IP en OSI-model[35]



De headergegevens in lagen 2 tot en met 7 worden 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 wordt 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.

[35] Bron: http://www2.themanualpage.org/networks/networks_osi2.php3.

2.3 Overzicht doeleinden

T-Mobile verklaart dat er (limitatief) drie doeleinden zijn voor de toepassing van data-analysetechnieken in haar mobiele netwerk.

1.	**Netwerkbeheer en het waarborgen van netwerkintegriteit en -veiligheid** (daaronder mede begrepen het voorkomen van congestie).[36] Om inzicht te hebben/krijgen in welke soorten diensten (apps/websites etc.) welke hoeveelheid capaciteit innemen op de verschillende delen van het netwerk[37] (hierna: netwerkplanning en -beheer), het oplossen en voorkomen van netwerkproblemen, om gevaren van buitenaf tijdig te detecteren als gevolg van de toegenomen invloed van hackers[38] (virussen, malware) en om ongeoorloofd gebruik of misbruik van het datanetwerk te voorkomen/bestrijden[39] (het handhaven van de *Fair Use Policy*).[40]
2.	Het oplossen van technische incidenten, en klantproblemen in individuele gevallen (***troubleshooting***).[41]
3.	**Optimalisatie van de dienstverlening aan klanten**.[42] Onder andere door video-compressie en *"ter naleving van de Europese roaming[43] regulering (speeddown na bereik van een maximum bedrag)"*[44] en van verplichtingen voortvloeiend uit de telecommunicatiewetgeving.[45]

T-Mobile verklaart dat zij data-analysetechnieken niet gebruikt om een differentiatie te kunnen aanbrengen in haar dienstenaanbod, dat wil zeggen om bepaalde diensten om andere redenen dan in verband met netwerkbeheer of het waarborgen van netwerkintegriteit te blokkeren of afwijkend te tariferen.[46]

In het nieuwste Privacy Statement (versie december 2012) van T-Mobile wordt opgemerkt over spamfiltering: *"T-Mobile heeft een geavanceerd netwerk wat ons in staat stelt om snel in te springen op technische ontwikkelingen en om jou een optimale internetervaring te bieden en tegelijkertijd je te beschermen tegen ongewenste praktijken zoals virussen en spam."* T-Mobile heeft spamfiltering gedurende het onderzoek niet

[36] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1. Zie ook reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2 en Zienswijze 1 T-Mobile, randnummer 6.
[37] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[38] Idem.
[39] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1.
[40] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[41] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1-2. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2. Idem, p. 4.
[42] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1-2. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[43] Te weten: de situatie waarin een bepaalde telecommunicatiedienst wordt voortgezet hoewel de gebruiker zich niet in het netwerk bevindt waarin deze geregistreerd staat (dat wil zeggen: daar waar hij klant is). Dankzij roaming kan hij met zijn mobiele (prepaid of postpaid) telefonie en/of data abonnement ook in het buitenland bellen/gebruik maken van mobiele datadiensten. Een toelichting op roaming is te lezen op: URL: http://nl.wikipedia.org/wiki/Roaming (URL laatst bezocht op 29 mei 2013).
[44] Brief T-Mobile van 19 september 2011, p. 2.
[45] Zienswijze 1 T-Mobile, randnummer 6.
[46] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1.

genoemd als concreet doel van de gegevensverwerking en heeft hierover ook geen informatie aan het CBP verstrekt. Dit doel is daarom niet door het CBP onderzocht.

Hierna worden achtereenvolgens beschreven de gegevensverwerkingen voor de hierboven genoemde drie doeleinden.

2.4 Netwerkbeheer en -integriteit

Als eerste verzamel- en verwerkingsdoeleinde van gegevens noemt T-Mobile netwerkbeheer en het waarborgen van netwerkintegriteit en -veiligheid (daaronder mede begrepen het voorkomen van congestie) (hierna: netwerkbeheer en -integriteit).[47]

Aanleiding toepassing data-analysetechnieken netwerkbeheer

T-Mobile verklaart dat de inzet van data-analysetechnieken noodzakelijk is: *"De verkeersstromen over het mobiele netwerk moet constant bewaakt worden om te voorkomen dat de continuïteit van de dienstverlening aan onze 4,5 miljoen klanten in gevaar komt. Hierbij is het van belang om te realiseren dat er wezenlijke verschillen zijn in het beheer van een mobiel netwerk ten opzichte van het beheer van een vast netwerk. In een vast netwerk is de verbinding naar de eindgebruiker exclusief voor deze eindgebruiker. Bij een mobiel netwerk wordt een deel van de verbinding gedeeld met alle eindgebruikers die zich binnen een bepaald geografisch gebied bevinden. De laatste schakel, de verbinding tussen een antenne-opstelpunt en de terminal van de eindgebruiker (telefoontoestel, USB-datastick, tablet, etc.) gaat via de ether en heeft fysische beperkingen. Er kan slechts een aantal verbindingen gelijktijdig opgezet worden en er is een beperkte datacapaciteit mogelijk om via de draadloze verbinding te versturen. Als een eindgebruiker klaar is met zijn/haar verbinding wordt de verbinding vrijgemaakt voor een nieuwe eindgebruiker. Een draadloze verbinding vraagt dus per definitie extra beheer om zo efficiënt mogelijk met de beperkingen vanuit de techniek om te gaan"*, (onderstreping toegevoegd door het CBP).[48]

Volgens T-Mobile maakt de (razend)snelle ontwikkeling en het gebruik van smartphones het noodzakelijk voor de mobiele telecommunicatiesector om de gevolgen daarvan voor het mobiele netwerk extra te managen.[49] T-Mobile geeft aan dat haar ervaring leert dat de beschikbaarheid van het mobiele netwerk kan worden beïnvloed door één applicatie.[50]

T-Mobile licht toe, aan de hand van een voorbeeld: *"[VERTROUWELIJK] Het gevolg hiervan was dat het T-Mobile netwerk overbezet raakte en de continuïteit van de verkeersstromen in gevaar kwamen als gevolg van congestie."*[51]

Mobiele apparaten, zoals smartphones (en daarop geïnstalleerde/gebruikte apps), maken ander(s) gebruik van het mobiele netwerk dan reguliere toestellen. Ze maken

[47] Idem. Zie ook reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2 en Zienswijze 1 T-Mobile, randnummer 6.
[48] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 1.
[49] Idem, p. 2. T-Mobile geeft aan dat ook de toegenomen invloed van hackers voor T-Mobile een belangrijke reden is om data-analysetechnieken in te zetten. Idem.
[50] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 1. T-Mobile voegt daaraan toe: [VERTROUWELIJK]. Idem, p. 2.
[51] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.

veel vaker contact met het internet, en gebruiken daarvoor telkens het signaleringskanaal (en het radiotoegangsnetwerk).[52] Zo verbreken smartphones veelvuldig de verbinding om de batterij te sparen. Er zijn apps die vaak weer verbinding (doen) zoeken met het netwerk, om gegevens te verversen door data van de server af te halen of te checken of er updates beschikbaar zijn. 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- of UMTS-gedeelte kan er ook niet meer worden gebeld.

Ten aanzien van de term "chatty apps" vult T-Mobile in haar zienswijze 2 aan dat het populaire spelletje Angry Birds dat 2.422 keer per uur contact zoekt met het netwerk, een bekend voorbeeld is van zo'n chatty app. Uitgaande van de verwachte toename van het aantal actieve apps (schattingen lopen op tot 48 miljard in 2015) betekent dat volgens T-Mobile een exponentiële toename van het netwerkverkeer. Om in die context stabiliteit en betrouwbaarheid van het netwerk te kunnen waarborgen moet voortdurend en gedetailleerd worden gevolgd op welke wijze gebruik wordt gemaakt van het netwerk en wat daarvan de implicaties zijn.[53]

T-Mobile schrijft in dat verband: *"Daarnaast genereren grote aantallen applicaties veel interactie en berichten met het netwerk in "idle mode" (met andere woorden: zonder dat de klant de applicatie daadwerkelijk gebruikt)."*[54]

T-Mobile noemt als voorbeeld: *"[VERTROUWELIJK]"*[55]

De informatie over welke apps op welke smartphones (met welke besturingssystemen) tot veel signaleringen in het mobiele netwerk leiden, is volgens T-Mobile aldus nodig om een voorspelling te kunnen doen van de benodigde capaciteit in het netwerk.

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 T-Mobile toe: *"Daarnaast zijn bestaande applicaties onderhevig aan constante ontwikkelingen die het gedrag van de applicatie volledig aanpast (bijv. na een update). Apple komt bijvoorbeeld regelmatig met een nieuwe OS release die op een specifieke dag beschikbaar wordt gesteld voor download. Elke OS release komt met nieuwe functionaliteiten (bijv. iCloud in iOS5.0) die door T-Mobile kwalitatief en kwantitatief geanalyseerd moet worden om de impact op het netwerk te bepalen. Indien nodig wordt meer capaciteit bijgebouwd voordat nieuwe Operating Systems live gaan."*[56]

[52] 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).
[53] Zienswijze 2 T-Mobile, p. 5.
[54] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 2.
[55] Idem, p. 1-2.
[56] Idem, p. 1.

T-Mobile heeft tijdens het onderzoek ter plaatse van 17 oktober 2011 verklaard dat met de data-analyse apparatuur actuele beheerrapportages worden gemaakt over de netwerkbelasting, zodat tijdig netwerkcapaciteit kan worden bijgeschakeld.[57]

T-Mobile verklaart in reactie op een verzoek om inlichtingen over de inzet van data-analysetechnieken in haar mobiele netwerk: *"[VERTROUWELIJK]"*[58]

Volgens T-Mobile kan niet worden volstaan met steekproefsgewijze controle: *"Het steekproefsgewijs meten dan wel regelmatig marktonderzoek doen onder smartphone gebruikers is niet afdoende om de populariteit van applicaties in te schatten. [VERTROUWELIJK] De smartphones applicaties komen met een dermate grote snelheid en hoeveelheid beschikbaar dat een steekproef of marktonderzoek niet afdoende betrouwbaar is om de netwerkcapaciteit en -kwaliteit te kunnen waarborgen. (…) [VERTROUWELIJK]"*, (onderstreping toegevoegd door het CBP).[59]

Desgevraagd verklaart T-Mobile dat een alternatieve vorm van data-analyse, waarbij alleen naar OSI-lagen 2 en 3 wordt gekeken, tekortschiet: *"Op L2 en L3 zijn bijvoorbeeld geen effecten op de radio interface* [dat wil zeggen: de radioweg, toevoeging door het CBP] *te herkennen die veroorzaakt worden door een zeer specifieke applicatie."*[60]

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.[61] 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).[62] Ter relativering van het belang en de mogelijkheden van zulke initiatieven wijst T-Mobile er in haar zienswijzen (evenwel) op dat hieruit (hooguit) kan worden opgemaakt dat er als gevolg van de snel

[57] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[58] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 5.
[59] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 2.
[60] Idem, p. 1.
[61] 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).
http://www.lightreading.com/document.asp?doc_id=208775.
[62] GSM Association, 'GSMA Announces New Initiatives Focusing On Creating More Efficient Mobile Applications', 27 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).

toenemende databehoeftes van smartphone- en tabletgebruikers op dit moment sprake is van een exponentieel toenemende druk op het signaleringsnetwerk.[63]

Het CBP stelt verder vast dat het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, (de gevolgen van) de toename van het datavolume relativeert in de 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 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."*[64] T-Mobile wijst (echter) onder andere op de continuïteitsverplichtingen en de afspraken die inmiddels[65] zijn gemaakt tussen KPN, T-Mobile en Vodafone om het telefoon- en sms-verkeer van elkaar over te nemen bij een storing. Zo'n toename van het verkeersvolume kan alleen worden opgevangen als het netwerkverkeer voortdurend wordt gemonitoord.[66]

Omdat netwerkproblemen kunnen worden veroorzaakt door enkele gebruikers, en in voorkomende gevallen alleen kunnen worden opgelost door deze individueel te benaderen, kan daarvoor niet worden volstaan met onomkeerbaar geanonimiseerde gegevens, aldus T-Mobile.[67] Om dat te illustreren heeft T-Mobile gewezen op [VERTROUWELIJK].

Data-analyse apparatuur

T-Mobile gebruikt(e) ten minste [VERTROUWELIJK] verschillende soorten data-analyse apparatuur (meetapparaten) voor het doeleinde netwerkbeheer en -integriteit. Het gaat om de **[VERTROUWELIJK: apparatuur]** van de [VERTROUWELIJK] leverancier [VERTROUWELIJK].[68]

[VERTROUWELIJK]

[63] Zienswijze 2 T-Mobile, p. 4.
[64] 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. Het citaat kwam ook voor in: BEREC Guidelines for Quality of Service in the scope of Net Neutrality. Draft for public consultation, dated 29 May 2012, p. 17. URL: http://berec.europa.eu/files/news/bor_12_32_guidelines.pdf (URL's laatst bezocht op 29 mei 2013).
[65] Zie o.a. *Kamerstukken II* 2012/13, 24 095, nr. 342 en 'Telecomproviders nemen dekking over bij storingen', *Nieuwsbericht Rijksoverheid* 7 mei 2013. URL: http://www.rijksoverheid.nl/nieuws/2013/05/07/telecomproviders-nemen-dekking-over-bij-storingen.html (URL laatst bezocht op 29 mei 2013).
[66] Zienswijze 2 T-Mobile, p. 4. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 7.
[67] Zienswijze 2 T-Mobile, p. 4. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 7.
[68] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3 en reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, bijlage 1. 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.

De [VERTROUWELIJK: apparatuur] wordt door T-Mobile [VERTROUWELIJK] gebruikt voor monitoring van verkeersstromen[69] (dat wil zeggen: door middel van actuele beheerrapportages over de netwerkbelasting, zodat tijdig netwerkcapaciteit kan worden bijgeschakeld, en bij (netwerk)testen met een reeks testnummers[70]), om gevaren van buitenaf tijdig te detecteren (virussen, malware)[71] en om ongeoorloofd gebruik of misbruik van het datanetwerk te voorkomen/bestrijden[72] (het handhaven van de *Fair Use Policy*).[73]

Uit (product)specificaties bij de [VERTROUWELIJK: apparatuur] volgt dat de data-analyse apparatuur in staat is om: [VERTROUWELIJK].

A. Netwerkplanning en -beheer

De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze met behulp van vooraf gedefinieerde en ingestelde filtermodules[74] gegevens verzamelt, vastlegt en bewaart[75] over het bezoek aan en gebruik van apps, websites en protocollen, zoals [VERTROUWELIJK].[76]

T-Mobile geeft in haar zienswijze 1 aan dat deze gegevens *"in enkele gevallen worden (…) verwerkt op het niveau van individuele eindgebruikers [VERTROUWELIJK]"*[77]

De [VERTROUWELIJK: apparatuur] herkent/identificeert (voor zover zij die websites bezoeken of apps en protocollen gebruiken) **potentieel** [VERTROUWELIJK] vooraf gedefinieerde apps, protocollen en services, zoals http (hostnames en URL's), https, ftp, [VERTROUWELIJK], file sharing [VERTROUWELIJK], VOIP, streaming applications [VERTROUWELIJK].[78]

Technisch vindt de data-analyse door T-Mobile als volgt plaats.

Data- en signaleringsverkeer packets van alle T-Mobile abonnees worden realtime 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 protocollen worden verkregen aan de hand van [VERTROUWELIJK].

T-Mobile verzamelt (aldus) aan de hand van de [VERTROUWELIJK] van al haar abonnees met een (prepaid of postpaid) data abonnement, bijvoorbeeld enerzijds het

---

[69] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3. "*Op basis van netwerk monitoring wordt bijvoorbeeld bekeken wat op dat moment de populairste Apps en meest bezochte websites zijn. [VERTROUWELIJK].*" Idem, p. 5.
[70] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011. De inzet van data-analysetechnieken voor (netwerk)testen, met een reeks testnummers valt buiten de scope van dit onderzoek.
[71] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[72] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1.
[73] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[74] Zienswijze 1 T-Mobile, randnummer 26.
[75] Zie idem, randnummer 26 en Annex, p. 14-16; reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2012 met kenmerk [VERTROUWELIJK], p. 1-2.
[76] Zienswijze 1 T-Mobile, Annex, p. 14-16 en [VERTROUWELIJK].
[77] Zienswijze 1 T-Mobile, randnummer 26.
[78] [VERTROUWELIJK].

MSISDN (06-nummer)[79] en anderzijds het IP-adres van-naar met poortnummer/gebruikt protocol[80], evenals aantallen bytes (volume)[81] en starttijd en eindtijd sessie.[82] Ten aanzien van het http-protocol en e-mailverkeer verzamelt T-Mobile tevens de hostname (URL op hoofddomein) en de URL van de website[83] respectievelijk [VERTROUWELIJK] het e-mailadres van de T-Mobile abonnee die met een e-mailaccount van een (andere) provider mailt of een derde die een T-Mobile klant mailt).[84]

T-Mobile schrijft in haar zienswijze 1: *"*[VERTROUWELIJK] *T-Mobile heeft daarom technische maatregelen genomen om de identificerende gegevens,* [VERTROUWELIJK] *ontoegankelijk te maken. Dit heeft zij gedaan door* [VERTROUWELIJK]. *Pas na anonimisering en aggregatie kunnen T-Mobile medewerkers deze data inzien via* [VERTROUWELIJK]*."*[85]

Vervolgens worden deze gegevens over websitebezoek en app- en protocolgebruik zonder het [VERTROUWELIJK] (MSISDN) opgeslagen in een achterliggende database. Deze gegevens worden gedurende een periode van ten hoogste veertien dagen bewaard.[86]

T-Mobile voegt toe over de [VERTROUWELIJK] dat aan de hand van [VERTROUWELIJK] de volgende gegevens worden geabstraheerd: het volume aan verbruikte data per klant ([VERTROUWELIJK) (MSISDN) per aggregatieperiode.[87]

Daarnaast worden dus aan de hand van de [VERTROUWELIJK] de volgende gegevens geabstraheerd: verbruikte datavolume per top subscriber (heavy user abonnee) per uur en per dag.[88] [VERTROUWELIJK]

T-Mobile schrijft dat er "[VERTROUWELIJK] *Deze gegevens worden maximaal 45 dagen bewaard",* (onderstreping toegevoegd door het CBP).[89]

---

[79] De categorie [VERTROUWELIJK]. Idem, Annex, p. 15.
[80] Bijvoorbeeld de categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 15 en [VERTROUWELIJK]. T-Mobile verklaart ten aanzien van het IP-adres van de smartphone: *"T-Mobile kent een klant - per opgezette sessie - een nieuw IP-adres toe. [VERTROUWELIJK]."* Brief T-Mobile van 19 september 2011, p. 2. De vraag of er sprake is van herleidbaarheid van IP-adressen van T-Mobile abonnees is niet door het CBP onderzocht. De inzet van data-analysetechnieken valt buiten de scope van dit onderzoek voor zover het deze IP-adressen betreft.
[81] Bijvoorbeeld de categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 16 en [VERTROUWELIJK].
[82] Bijvoorbeeld de categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 16 en [VERTROUWELIJK].
[83] De categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 16 en [VERTROUWELIJK].
[84] De categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 16 en [VERTROUWELIJK]. Vgl. ook [VERTROUWELIJK].
[85] Zienswijze 1 T-Mobile, Annex, p. 15-16.
[86] Idem, Annex, p. 15-16 en [VERTROUWELIJK].
[87] [VERTROUWELIJK].
[88] Zienswijze 1 T-Mobile, Annex, p. 16. [VERTROUWELIJK].
[89] Zienswijze 1 T-Mobile, Annex, p. 16. Of T-Mobile een grondslag heeft voor de inzet van data-analysetechnieken ten behoeve van (handhaving van) de Fair Use Policy is niet door het CBP beoordeeld.

Via een gebruikersinterface kunnen onder andere de volgende geaggregeerde gegevens worden geraadpleegd: [VERTROUWELIJK].[90]

T-Mobile verklaart in reactie op een verzoek om inlichtingen over de opslag van de gegevens: "[VERTROUWELIJK]."[91]

Ten slotte kunnen de daartoe bevoegde T-Mobile medewerkers rapportages uitdraaien met deze gegevens uit de gebruikersinterface[92] [VERTROUWELIJK].[93]

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

B. Ongewenst dataverkeer

Daarnaast inspecteert en analyseert T-Mobile met de [VERTROUWELIJK: apparatuur] het dataverkeer (inclusief signaleringsverkeer)[94] van al haar abonnees met een (prepaid of postpaid) data abonnement teneinde ongewenst dataverkeer (virussen, malware) tegen te houden.[95]

Het is (ook) volgens het CBP algemeen aanvaard dat internet aanbieders naar de inhoud van e-mails moeten kijken (naar de data-inhoud van packets) om virussen en malware te kunnen herkennen. Bij de bestrijding van virussen en malware worden over het algemeen lijsten gebruikt met de 'fingerprints' (vooraf gedefinieerde herkenningspatronen), die worden opgesteld door gespecialiseerde securitybedrijven. Om nieuwe, nog niet-geïnventariseerde virussen en malware te kunnen herkennen in de bijlagen van e-mails zijn heuristische (zelflerende) technieken nodig die (inhoudelijk) in bestanden kijken naar kwaadaardige code.[96]

T-Mobile schrijft in haar zienswijze 1 dat zij voor dit doeleinde (ook) gebruik maakt van [VERTROUWELIJK] De gegevens worden bewaard zolang dit nodig is om de aard en oorsprong van de aanval te kwalificeren (ten hoogste veertien dagen).[97]

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit 'subdoeleinde' virus- en malwarebestrijding verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

---

[90] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[91] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 1.
[92] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011. Vgl. ook o.a. [VERTROUWELIJK].
[93] Zienswijze 1 T-Mobile, randnummer 27 en Annex, p. 16.
[94] Daaronder begrepen inhoud van door abonnees (gedownloade) bestanden en ontvangen e-mails aan de hand vooraf gedefinieerde virus- en malwareherkenningspatronen, voor zover nodig om virussen/malware tegen te houden en te verwijderen (oftewel, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer).
[95] Zie o.a. reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 2, zienswijze T-Mobile, Annex, p. 14 en [VERTROUWELIJK].
[96] Een toelichting op virusbestrijdingstechnieken is te lezen op URL: http://en.wikipedia.org/wiki/Antivirus_software (URL laatst bezocht op 28 mei 2013).
[97] Zienswijze 1 T-Mobile, Annex, p. 15.

C. Fair Use Policy en T-Mobile HotSpot in de trein

Ten slotte gebruikt T-Mobile de [VERTROUWELIJK: apparatuur] om ongeoorloofd gebruik of misbruik van het datanetwerk te voorkomen/bestrijden[98] (het handhaven van de *Fair Use Policy*[99] of een Speed Step Down, bijvoorbeeld na een bepaald gebruik[100]) alsmede in het kader van T-Mobile HotSpot in de trein.[101]

[VERTROUWELIJK]

Fair Use Policy

T-Mobile geeft in haar zienswijze 1 aan dat zij voor dit doeleinde gebruik maakt van [VERTROUWELIJK]. T-Mobile geeft aan dat aan de hand van [VERTROUWELIJK] de volgende gegevens worden geabstraheerd: het volume aan verbruikte data[102] per klant ([VERTROUWELIJK: identifier]) per aggregatieperiode.[103] T-Mobile licht in haar zienswijze 1 toe dat [VERTROUWELIJK]. Zit de gebruiker boven een bepaalde *threshold* (wettelijk, of op basis van zijn abonnement) dan [VERTROUWELIJK] een signaal naar de [VERTROUWELIJK: apparatuur], die de vereiste actie onderneemt (zoals een Speed Step Down naar [VERTROUWELIJK] of het blokkeren van toegang tot het internet in geval van roaming).[104]

De gegevens geabstraheerd aan de hand van [VERTROUWELIJK] worden maximaal 45 dagen bewaard.[105]

T-Mobile HotSpot in de trein

T-Mobile blokkeert via de [VERTROUWELIJK: apparatuur] bepaalde diensten, zoals peer-to-peer verkeer, [VERTROUWELIJK], streaming [VERTROUWELIJK] bij (het gebruik van) NS Free Hotspot.[106]

AFBEELDING 2 Grafische interface [VERTROUWELIJK: apparatuur], geblokkeerde protocollen[107] [VERTROUWELIJK]

T-Mobile verwijst daarbij naar artikel 3.7 van de algemene voorwaarden die gebruikers accepteren wanneer ze gebruik maken van de gratis WiFi Hotspots: *"Peer-to-peer verkeer en streaming zijn niet mogelijk via T-Mobile HotSpot. De download- en uploadsnelheid van file transfer (FTP) wordt beperkt tot 128Kbps."*[108]

T-Mobile licht (nader) toe: [VERTROUWELIJK]

---

[98] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1.
[99] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[100] Zienswijze 1 T-Mobile, Annex, p. 14.
[101] Idem, Annex, p. 13 en 17.
[102] Bijvoorbeeld de categorieën [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 14 en 16 en [VERTROUWELIJK].
[103] Idem, Annex, p. 13 en 17.
[104] Idem, Annex, p. 16.
[105] Zienswijze 1 T-Mobile, Annex, p. 13. Of T-Mobile een grondslag heeft voor de inzet van data-analysetechnieken ten behoeve van (handhaving van) de Fair Use Policy wordt/is niet door het CBP beoordeeld.
[106] Mondelinge verklaring T-Mobile en print-outs T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011. Vgl. ook o.a. [VERTROUWELIJK].
[107] Print-out T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011, 1-5.
[108] Zienswijze 1 T-Mobile, Annex, p. 17.

De vraag of er sprake is van herleidbaarheid van gebruikers van T-Mobile HotSpot in de trein is niet door het CBP onderzocht. De inzet van data-analysetechnieken valt buiten de scope van dit onderzoek voor zover het T-Mobile HotSpot in de trein betreft.

[VERTROUWELIJK]

Oplossen en voorkomen van netwerkproblemen

T-Mobile heeft de [VERTROUWELIJK: apparatuur] in 2006 aangekocht.[109] De [VERTROUWELIJK: apparatuur] is sinds 2007 'vol in bedrijf'.[110]

De [VERTROUWELIJK: apparatuur] wordt door T-Mobile [VERTROUWELIJK] gebruikt voor het monitoren van het netwerk/*handset performance*[111], om connectiviteit op het netwerk van T-Mobile mee te monitoren en te beheren (service management en het bewaken van service levels).[112]

Uit (product)documentatie bij de [VERTROUWELIJK: apparatuur] volgt dat de data-analyse apparatuur, zoals gebruikt door T-Mobile, in staat is om: [VERTROUWELIJK].

De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze door T-Mobile wordt gebruikt om connectiviteit op het netwerk van T-Mobile mee te monitoren en te beheren.[113] [VERTROUWELIJK].

T-Mobile benadrukt in haar zienswijze 1 dat het gebruik van de [VERTROUWELIJK: apparatuur] slechts betrekking heeft op gegevens betreffende de geslaagde en niet-geslaagde pogingen van abonnees en eindgebruikers (randapparatuur) om gebruik te maken van het netwerk van T-Mobile.[114]

T-Mobile verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement, bijvoorbeeld enerzijds het [VERTROUWELIJK: identifiers] en anderzijds [VERTROUWELIJK] handset performance (waaronder [VERTROUWELIJK]), en tijdsvenster [VERTROUWELIJK].[115]

Vervolgens werden deze gegevens bij aanvang van het onderzoek per abonnee opgeslagen [VERTROUWELIJK] en op verschillende aggregatieniveaus (vijftien minuten-, dag-, week- en maandbasis) gedurende respectievelijk dertig dagen, veertig dagen, één jaar en twee jaar bewaard.[116]

---

[109] [VERTROUWELIJK].
[110] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[111] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3.
[112] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[113] Zienswijze 1, Annex, p. 18.
[114] Zienswijze 1 T-Mobile, randnummer 31.
[115] Zienswijze 1 T-Mobile, Annex, p. 18-19. Zie ook [VERTROUWELIJK], p. 5 e.v. en [VERTROUWELIJK], p. 5 e.v. [VERTROUWELIJK].
[116] Brief T-Mobile van 19 september 2011, p. 2, reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3, reactie T-Mobile op vordering van het CBP van 21 februari 2013, p. 7.

T-Mobile licht toe: *"[VERTROUWELIJK]."*[117]

Met het begrip 'aggregatie' doelt T-Mobile hier (ook) op het combineren (aggregeren) van gegevens per abonnee over een langere periode.

Via een (gebruikers)interface kunnen onder andere de volgende gegevens worden geraadpleegd: [VERTROUWELIJK].

AFBEELDING 3 Grafische interface [VERTROUWELIJK: apparatuur], [VERTROUWELIJK][118]
[VERTROUWELIJK]

Getroffen maatregelen
T-Mobile heeft gedurende het onderzoek de bewaartermijnen voor wat betreft de verschillende aggregatieniveaus verkort tot:

- 15 dagen (op 15 minuten basis geaggregeerde data);
- 15 dagen (op dagbasis geaggregeerde data); en
- 14 dagen (op weekbasis geaggregeerde data).[119]

[VERTROUWELIJK]

[VERTROUWELIJK]

Oplossen en voorkomen van netwerkproblemen

De [VERTROUWELIJK: apparatuur][120] wordt door T-Mobile [VERTROUWELIJK] gebruikt om netwerk issues te voorkomen en voor incident management (*network outages*).[121]

Uit (product)documentatie bij de [VERTROUWELIJK: apparatuur] volgt dat de data-analyse apparatuur in staat is om: [VERTROUWELIJK]

De [VERTROUWELIJK: apparatuur] heeft als instelling dat [VERTROUWELIJK] gegevens verzamelt, vastlegt en bewaart[122] over het functioneren van het mobiele netwerk [VERTROUWELIJK] om netwerkproblemen en -incidenten te voorkomen/op te lossen, waaronder [VERTROUWELIJK] performance informatie/status.[123]

---

[117] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3. Vgl. o.a. [VERTROUWELIJK] Product Description [VERTROUWELIJK], p. 14: *"[VERTROUWELIJK]."*
[118] Printout T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011, 3-5.
[119] Reactie T-Mobile op vordering van 21 februari 2013, p. 7-8.
[120] Te weten: de [VERTROUWELIJK: apparatuur].
[121] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[122] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 1, reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3 en print-outs T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[123] Print-out T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011, 5-5 ([VERTROUWELIJK] - network monitoring).

T-Mobile verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement bijvoorbeeld gegevens over [VERTROUWELIJK].[124]

T-Mobile verklaart: *"[VERTROUWELIJK]."*[125]

Vervolgens worden deze gegevens in de achterliggende database(s)/bestanden opgeslagen en gedurende ten hoogste veertien dagen bewaard.[126]

Via een gebruikersinterface kunnen onder andere de volgende gegevens worden geraadpleegd: [VERTROUWELIJK].

AFBEELDING 4 Grafische interface [VERTROUWELIJK: apparatuur][127]

[VERTROUWELIJK]

Tijdens het onderzoek ter plaatse van 17 oktober 2011 heeft het CBP in de gebruikersinterface geen voorbeelden aangetroffen [VERTROUWELIJK].[128]

[VERTROUWELIJK: apparatuur]
T-Mobile heeft een pilot gedaan met de [VERTROUWELIJK: apparatuur] van maart tot en met juni 2011.[129] T-Mobile heeft de data-analyse apparatuur naderhand aangeschaft.[130]

De [VERTROUWELIJK: apparatuur] is gedurende de pilot gebruikt en zal door T-Mobile [VERTROUWELIJK] worden gebruikt voor netwerkplanning.[131] Tijdens het onderzoek ter plaatse van 17 oktober 2011 was de [VERTROUWELIJK: apparatuur] niet in gebruik. [VERTROUWELIJK]

Uit (product)documentatie bij de [VERTROUWELIJK: apparatuur] volgt dat de data-analyse apparatuur in staat is om: [VERTROUWELIJK].

[124] Idem.
[125] Reactie T-Mobile op verzoek om inlichtingen van 24 oktober 2011 met kenmerk [VERTROUWELIJK], p. 1.
[126] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3. Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[127] Print-out T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011, [VERTROUWELIJK: apparatuur].
[128] De vraag of er sprake is van herleidbaarheid van de gegevens die T-Mobile verzamelt met behulp van de [VERTROUWELIJK: apparatuur] is niet door het CBP onderzocht. De inzet van data-analysetechnieken valt buiten de scope van dit onderzoek voor zover het de [VERTROUWELIJK: apparatuur] betreft.
[129] Reactie T-Mobile op verzoek om inlichtingen van 19 oktober 2011, p. 2 en mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.
[130] Idem. [VERTROUWELIJK] van 18 oktober 2011.
[131] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011.

Netwerkplanning en -beheer

De [VERTROUWELIJK: apparatuur] heeft volgens de (product)documentatie als fabrieksinstelling dat deze met behulp van vooraf gedefinieerde en ingestelde filtermodules gegevens verzamelt, vastlegt en bewaart[132] over het gebruik van protocollen en applicaties, zoals [VERTROUWELIJK].

De [VERTROUWELIJK: apparatuur] herkent/identificeert (onder andere afhankelijk of zij die websites bezoeken of apps en protocollen gebruiken) volgens de (product)documentatie protocollen en applicaties, zoals [VERTROUWELIJK].[133]

Met behulp van de [VERTROUWELIJK: apparatuur] kunnen volgens de (product)specificaties (alsdan) worden verzameld, bijvoorbeeld enerzijds [VERTROUWELIJK: identifiers] en anderzijds de hostname (URL op hoofddomein)[134], [VERTROUWELIJK], evenals aantallen bytes [VERTROUWELIJK][135] en tijdsvenster.[136]

Vervolgens worden volgens de (product)specificaties deze gegevens per abonnee in de achterliggende database/bestanden opgeslagen en bewaard.[137]

Via een gebruikersinterface[138] kunnen volgens de (product)specificaties onder andere de volgende gegevens worden geraadpleegd: [VERTROUWELIJK].[139]

Ten slotte kan T-Mobile volgens de (product)specificaties rapportages uitdraaien [VERTROUWELIJK].[140]

De feitelijke instellingen van de [VERTROUWELIJK: apparatuur] en de wijze waarop deze is geïmplementeerd in het mobiele netwerk van T-Mobile is niet door het CBP onderzocht. De inzet van data-analysetechnieken valt buiten de scope van dit onderzoek voor zover het de [VERTROUWELIJK: apparatuur] betreft.

(Algemene) technische en organisatorische maatregelen

T-Mobile verklaart in reactie op een verzoek om inlichtingen van OPTA een combinatie van technische en organisatorische maatregelen te hanteren, waaronder Global Security Policies gebaseerd op de ISO27001 standaard voor Information Security Management Systeem en een Privacy Code of Conduct van moedermaatschappij Deutsche Telekom AG, toegangsautorisaties (slechts een selecte groep medewerkers heeft toegang tot gebruik van de data analyse apparatuur), toegangsbeveiliging door middel van [VERTROUWELIJK].[141]

T-Mobile voegt in haar zienswijze 1 daaraan toe dat ook voorzien is in andere technische en organisatorische beveiligingsmaatregelen om een zorgvuldige en

---

[132] Idem, p. 12 en 26.
[133] Idem, p. 18.
[134] Idem, p. 18.
[135] Zie o.a. idem, p. 6 [VERTROUWELIJK], 11 en 13 e.v.
[136] Vgl. idem, p. 18-19.
[137] Idem, p. 12 en 26.
[138] Vgl. idem, p. 10.
[139] Zie o.a. idem, p. 11, 14-15, 18 en 23.
[140] Vgl. idem, p. 12 en 22.
[141] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 3.

rechtmatige gegevensverwerking te waarborgen. Deze maatregelen betreffen een intern en extern (vanuit het moederbedrijf, en via onder andere externe audits) gehandhaafd beleid met betrekking tot functiescheidingen, beveiligingseisen, toegang tot applicaties en de verzamelde gegevens etc.[142]

Informatie voor abonnees

Het algemene Privacy Statement van T-Mobile (hierna: het oude Privacy Statement) bevat de volgende informatie over de verwerking van gegevens ten behoeve van netwerkbeheer en -integriteit, voor zover voor dit onderzoek van belang:

> *"T-Mobile bewaakt de continuïteit van haar mobiele netwerk. T-Mobile monitoort daarvoor niet jouw individuele gebruik van het netwerk maar onderzoekt wel of er bijvoorbeeld ergens in het netwerk van T-Mobile problemen voorkomen, bijvoorbeeld storingen of piekverbruik. (…)*
>
> *T-Mobile kan op basis van monitoring van je belgedrag overgaan tot het geven van een belbeperking voor bepaalde bestemmingen indien T-Mobile constateert dat er sprake is van exorbitant gebruik. T-Mobile streeft ernaar om je dergelijk gevallen vooraf persoonlijk telefonisch of per sms-bericht te informeren voordat tot een belbeperking wordt overgegaan. (…)",* (onderstreping toegevoegd door het CBP). [143]

Verder bevatten de 'Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument' en de 'Algemene Voorwaarden T-Mobile PrePaid' de volgende informatie:

> *"T-Mobile verwerkt Persoonsgegevens van haar Klanten voor de volgende doeleinden:*
> *(…) het analyseren van het gebruik van het Netwerk voor zover dat met het oog op het verkeersbeheer, het waarborgen, verbeteren van de continuïteit en kwaliteit van de dienstverlening en de verantwoorde bedrijfsvoering van T-Mobile noodzakelijk is*. (…)
>
> *De Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwezenlijking van de hiervoor genoemde doeleinden."*[144]

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

---

[142] Zienswijze 1 T-Mobile, randnummer 9.
[143] Privacy Statement April 2011.
[144] Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument (versies: geldig vanaf 31 mei en januari 2011) en Algemene Voorwaarden T-Mobile Abonnee Consument (geldig vanaf 10 mei 2010). Vgl. Algemene Voorwaarden T-Mobile PrePaid (geldig vanaf oktober 2010). URL: http://www.t-mobile.nl/corporate/htdocs/popup/voorwaarden.aspx (URL laatst bezocht op 29 mei 2013).

Getroffen maatregelen

T-Mobile heeft de privacyverklaring van het bedrijf aangepast, per april en december 2012.

Het nieuwe Privacy Statement (versie april 2012) van T-Mobile bepaalde, voor zover voor dit onderzoek van belang:

> *"Als gevolg van de soort dienstverlening beschikt T-Mobile over je persoonsgegevens. Waarvoor T-Mobile deze persoonsgegevens gebruikt, hoe zij de bescherming van je privacy en persoonsgegevens waarborgt en wat jouw rechten zijn met betrekking tot de verwerking van je persoonsgegevens kan je lezen in dit Privacy Statement. (…)*
>
> *Persoonsgegevens zijn onder te verdelen in gebruikersgegevens, verkeersgegevens en locatiegegevens. (…)*
>
> *Voorbeeld van gebruikersgegevens*
> *Voor het aanbieden van een abonnement is het noodzakelijk dat T-Mobile je naam, adres, woonplaats, geboortedatum en je bankgegevens (voor de facturering) registreert. Daarnaast kan T-Mobile bijv. ook je e- mailadres, afgenomen diensten of mobiele nummer registreren. Heb je een persoonlijke digitale omgeving (My T-Mobile of Mijn Online account) dan verwerkt T-Mobile ook je inlognaam en wachtwoord.*
>
> *Voorbeeld van verkeersgegevens*
> *Verkeersgegevens hebben betrekking op het daadwerkelijke gebruik van de afgenomen internet- of telefoniedienst. Zo registreert T- Mobile het tijdstip, de datum en de duur van de tot stand gekomen verbinding, het nummer dat je belt en de locatie. In het geval van gebruik van (mobiel) internet worden de begin- en eindtijd van de internetsessie en bijvoorbeeld ook het volume van het internetgebruik geregistreerd.*
>
> *Voorbeeld van locatiegegevens*
> *Locatiegegevens hebben betrekking op de plaats waar gebruik wordt gemaakt van je mobiele apparaat, bijvoorbeeld je mobiel of tablet. Deze gegevens worden verwerkt ten behoeve van wettelijke verplichtingen en voor het leveren van toegevoegde waarde diensten (zoals lokale weers- en verkeersdiensten), mits je daarvoor voorafgaand toestemming hebt gegeven.*
>
> *(…) De aanvraag voor een aansluiting en het overbrengen van de communicatie*
> *Allereerst verwerkt T-Mobile je persoonsgegevens voor de (uitvoering van de) dienst aan jou. Dat betekent onder meer voor het in behandeling nemen van je aanvraag, het aansluiten en opzetten van een verbinding en het sturen van een factuur voor de afgenomen diensten. (…)*
>
> *(…) Kwaliteit van de dienstverlening*
> *T-Mobile bewaakt de continuïteit en integriteit van haar mobiele –en vaste netwerken. T-Mobile onderzoekt daarvoor of er bijvoorbeeld ergens in het netwerk van T-Mobile problemen voorkomen, zoals storingen of piekverbruik. Daarnaast verwerkt T-Mobile verkeersgegevens om de kwaliteit van de dienstverlening te*

waarborgen en om je zo optimaal mogelijk van dienst te kunnen zijn. De verwerking van je persoonsgegevens is nodig om de diensten te leveren, maar ook om voortdurend te verbeteren en aan te passen aan jouw wensen. (…)

(…) Hoogverbruik
T-Mobile kan op basis van monitoring van je bel- en internetgedrag overgaan tot het beperken van bepaalde bestemmingen indien T-Mobile constateert dat er sprake is van exorbitant gebruik. T-Mobile streeft ernaar om je in dergelijke gevallen vooraf persoonlijk telefonisch of per sms-bericht te informeren voordat er tot een beperking wordt overgegaan.

(…) HOE LANG WORDEN JE PERSOONSGEGEVENS BEWAARD?
T-Mobile bewaart je persoonsgegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de doeleinden waarvoor T-Mobile je gegevens heeft verzameld. Hoe lang je gegevens worden bewaard is dus afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per (categorie van) gegeven(s) verschillen.

T-Mobile bewaart in ieder geval je persoonsgegevens gedurende de looptijd van je abonnement en conform de wettelijke verplichtingen zoals genoemd onder 3.7. van dit Privacy Statement [zoals de bewaarplicht verkeersgegevens, toevoeging door het CBP]."[145]

Het nieuwste Privacy Statement (versie december 2012) van T-Mobile bepaalt (verder), voor zover voor dit onderzoek van belang:

"Om de kwaliteit van de dienstverlening zo goed mogelijk te waarborgen en te optimaliseren, analyseert T- Mobile bepaalde gegevens over het gebruik van het netwerk. Denk hierbij aan bel-, sms- en internetgegevens, maar ook welk toestel je gebruikt en hoe dit toestel in ons netwerk functioneert, zoals het aantal succesvol opgezette verbindingen. Deze gegevens worden gebruikt voor beheer en beveiliging van ons netwerk en stelt ons in staat om te onderzoeken of er ergens in het netwerk problemen zijn, zoals storingen of piekverbruik.

T-Mobile heeft een geavanceerd netwerk wat ons in staat stelt om snel in te springen op technische ontwikkelingen en om jou een optimale internetervaring te bieden en tegelijkertijd je te beschermen tegen ongewenste praktijken zoals virussen en spam.[146]

---

[145] T-Mobile Privacy Statement (versie april 2012). URL: https://www.t-mobile.nl/Global/media/pdf/privacy_statement_juni_2012.pdf (URL laatst bezocht op 29 mei 2013).

[146] T-Mobile heeft spamfiltering gedurende het onderzoek niet genoemd als concreet doel van de gegevensverwerking. Dit doel is daarom niet door het CBP onderzocht. Wel geldt in het algemeen dat filtering van uitgaande spam naar het oordeel van het CBP noodzakelijk kan zijn voor een internet aanbieder om een wettelijke plicht (zorgplicht internetveiligheid: artikel 11.3 van de Tw) uit te voeren. Vgl. WP29 118. Opinion 2/2006 on privacy issues related to the provision of email screening services van 21 februari 2006, p. 7. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf (URL laatst bezocht op 29 mei 2013).

Om dit goed te kunnen doen houdt T-Mobile bij wat er gebeurt op haar netwerk. Hiervoor gebruiken we geavanceerde technieken die virussen kunnen herkennen, maar ook het gebruik van apps en toepassingen op ons netwerk en veelbezochte websites zien. Deze informatie kunnen wij gebruiken om bepaalde soorten verkeer voorrang te geven (zoals Skype) en verstoppingen te voorkomen, (…) en ons netwerk en onze klanten te beschermen tegen virussen, malware en andere aanvallen. Aan de hand van de informatie over het gebruik van applicaties en de bezochte websites kunnen we er voor zorgen dat er altijd genoeg capaciteit is om jou de diensten te leveren zoals je die van ons gewend bent.

Deze analyse-technieken worden ingezet op verschillende plaatsen in ons netwerk en in sommige gevallen worden daarbij gegevens verwerkt die betrekking hebben opjou, zoals je toestelnummer (IMEI) of mobiele nummer. Jouw privacy staat daarbij voorop: nadat de relevante informatie uit het netwerk is gehaald worden de gegevens direct geanonimiseerd. T-Mobile kijkt niet naar de inhoud van jouw berichten of de door jouw bezochte websites", (onderstreping toegevoegd door het CBP).[147]

2.5 Troubleshooting

Als tweede verzamel- en verwerkingsdoeleinde van gegevens noemt T-Mobile troubleshooting (dat wil zeggen: het oplossen van technische incidenten en klantproblemen in individuele gevallen).[148]

Aanleiding toepassing data-analysetechnieken troubleshooting

T-Mobile verklaart: "*In uitzonderlijk specifieke gevallen - veelal in direct overleg met de klant ten behoeve van het oplossen van een individueel probleem - kan voor trouble-shooting doeleinden dieper worden gekeken. Bij het analyseren van de verkeersstromen wordt echter niet gekeken naar de inhoud van berichten van de klant.*"[149]

Data-analyse apparatuur

T-Mobile gebruikt(e) [VERTROUWELIJK] data-analyse apparatuur in het kader van de afhandeling van klantklachten, ter ondersteuning van de klantenservice (te weten: de [VERTROUWELIJK: apparatuur].[150]

T-Mobile licht toe: *"[VERTROUWELIJK]"*[151]

[VERTROUWELIJK]

[147] T-Mobile Privacy Statement (versie december 2012). URL: https://www.t-mobile.nl/Global/media/pdf/privacy-statement.pdf (URL laatst bezocht op 29 mei 2013).
[148] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1-2. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2. Idem, p. 4.
[149] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[150] Mondelinge verklaring T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3. Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, bijlage 1.
[151] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 2.

AFBEELDING 5: Grafische interface klantenservice [VERTROUWELIJK: apparatuur], [VERTROUWELIJK][152]

[VERTROUWELIJK]

Via de gebruikersinterface ten behoeve van de klantenservice kunnen, in geval van de [VERTROUWELIJK: apparatuur], bijvoorbeeld de volgende gegevens worden geraadpleegd: [VERTROUWELIJK].

T-Mobile verklaart dat deze verwerking is gebaseerd op toestemming: *"Troubleshooting wordt gedaan op verzoek van dan wel in direct overleg met de klant voor het oplossen van een individueel probleem. (…)."*[153]

T-Mobile slaat voor dit doeleinde in sommige gevallen ook gegevens over het dataverkeer op.[154]

T-Mobile voegt daaraan toe: *"Bovendien informeert T-Mobile haar klanten in haar Privacy Statement, zoals vermeld op de T-Mobile website, ook over het feit dat zij continue onderzoek doet in haar netwerk om de kwaliteit van haar dienstverlening te waarborgen dan wel te verbeteren."*[155]

Informatie voor abonnees

De 'Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument' en de 'Algemene Voorwaarden T-Mobile PrePaid' bevatten de volgende informatie, voor zover voor dit onderzoek van belang:

> *"T-Mobile verwerkt Persoonsgegevens van haar Klanten voor de volgende doeleinden:*
> *(…) de inlichtingenverstrekking aan de Klant, klachtbehandeling en geschillenbeslechting* (…)."[156]

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

Getroffen maatregelen

Het nieuwe Privacy Statement (april 2012) van T-Mobile bepaalde, voor zover voor dit onderzoek van belang:

---

[152] Print-out T-Mobile tijdens het onderzoek ter plaatse van 17 oktober 2011, p. 4-5 ([VERTROUWELIJK: apparatuur]).
[153] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 4.
[154] Zie o.a. reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 4 en brief T-Mobile van 19 september 2011, p. 2.
[155] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 2.
[156] Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument (versies: geldig vanaf 31 mei en januari 2011) en Algemene Voorwaarden T-Mobile Abonnee Consument (geldig vanaf 10 mei 2010). Algemene Voorwaarden T-Mobile PrePaid (geldig vanaf oktober 2010).

> *"Allereerst verwerkt T-Mobile je persoonsgegevens voor de (uitvoering van de) dienst aan jou. Dat betekent onder meer voor het in behandeling nemen van je aanvraag, het aansluiten en opzetten van een verbinding en het sturen van een factuur voor de afgenomen diensten. Maar ook voor het afhandelen van jouw vragen en verzoeken over de dienst"*, (onderstreping toegevoegd door het CBP.)[157]

Het nieuwste Privacy Statement (versie december 2012) van T-Mobile bepaalt, voor zover voor dit onderzoek van belang:

> *"Om de kwaliteit van de dienstverlening zo goed mogelijk te waarborgen en te optimaliseren, analyseert T- Mobile bepaalde gegevens over het gebruik van het netwerk. Denk hierbij aan bel-, sms- en internetgegevens, maar ook welk toestel je gebruikt en hoe dit toestel in ons netwerk functioneert, zoals het aantal succesvol opgezette verbindingen. Deze gegevens worden gebruikt voor beheer en beveiliging van ons netwerk en stelt ons in staat om te onderzoeken of er ergens in het netwerk problemen zijn, zoals storingen of piekverbruik"*, (onderstreping toegevoegd door het CBP).[158]

2.6 Videocompressie

Als derde verzamel- en verwerkingsdoeleinde van gegevens noemt T-Mobile - onder meer[159] - optimalisatie van de dienstverlening aan klanten (videocompressie).[160]

Aanleiding toepassing data-analysetechnieken

T-Mobile verklaart dat de inzet van data-analysetechnieken voor dit doeleinde noodzakelijk is: *"Door de immense toename van - de mogelijkheden van - het mobiele dataverkeer welke sinds de introductie van het 3G netwerk heeft plaatsgevonden, is het noodzakelijk om verkeersstromen te analyseren voor de optimalisatie van de dienstverlening aan de T-Mobile klanten."*[161] En: *"(…) met behulp van verkeersstroom analyses kan T-Mobile bijvoorbeeld kijken naar de hoeveelheid mobiele gebruikers op het mobiele datanetwerk die Youtube.com bezoeken. (…) Bij zo'n analyse wordt dus niet gekeken welke video's op Youtube bekeken worden door de eindgebruikers, maar uitsluitend naar het totale datavolume."*[162]

T-Mobile licht toe, aan de hand van een voorbeeld: *"[VERTROUWELIJK]."*[163]

Data-analyse apparatuur

T-Mobile gebruikt [VERTROUWELIJK: apparatuur] van de leverancier [VERTROUWELIJK] voor videocompressie.[164]

---

[157] T-Mobile Privacy Statement (versie april 2012).
[158] T-Mobile Privacy Statement (versie december 2012).
[159] De inzet van data-analysetechnieken valt, zoals vermeld, buiten de scope van dit onderzoek voor zover het betrekking heeft op data roaming verkeer.
[160] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1-2. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[161] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2.
[162] Reactie T-Mobile op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.
[163] Idem. Zie ook reactie T-Mobile op verzoek om inlichtingen van 8 september, p. 5: *"[VERTROUWELIJK]."*

T-Mobile verklaart: *"T-Mobile optimaliseert video (afhankelijk van [VERTROUWELIJK] en van de door de gebruiker ingestelde setting). [VERTROUWELIJK", (*onderstreping toegevoegd door het CBP).[165]

Informatie voor abonnees

De 'Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument' en de 'Algemene Voorwaarden T-Mobile PrePaid' bevatten de volgende informatie over de verwerking van gegevens ten behoeve van optimalisatie van de dienstverlening, voor zover voor dit onderzoek van belang:

> *"T-Mobile verwerkt Persoonsgegevens van haar Klanten voor de volgende doeleinden:*
> *(…) het sluiten en uitvoeren van de Overeenkomst; (…)*
> *(…) het analyseren van het gebruik van het Netwerk voor zover dat met het oog op het verkeersbeheer, het waarborgen, verbeteren van de continuïteit en kwaliteit van de dienstverlening en de verantwoorde bedrijfsvoering van T-Mobile noodzakelijk is.* (…)"[166]

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

Op de 'Speed Instellingen pagina' op het toestel van de abonnee wordt de volgende informatie getoond: *"Om het gebruik van mobiel internet optimaal mogelijk te maken biedt T-Mobile geheel kosteloos de mogelijkheid om de snelheid van je mobiele internet te optimaliseren. Hieronder kun je aangeven wat jou gewenste instelling is. Aanbevolen is om 'Snelheid optimaliseren' te kiezen. Hiermee worden pagina's sneller geladen zonder dat je kwaliteit verliest. (…)"*[167]

Getroffen maatregelen

Het nieuwe Privacy Statement (versie april 2012) van T-Mobile bepaalde, voor zover voor dit onderzoek van belang:

> *(…) Kwaliteit van de dienstverlening*
> *(…) Daarnaast verwerkt T-Mobile verkeersgegevens om de kwaliteit van de dienstverlening te waarborgen en om je zo optimaal mogelijk van dienst te kunnen zijn. De verwerking van je persoonsgegevens is nodig om de diensten te leveren, maar ook om voortdurend te verbeteren en aan te passen aan jouw wensen.*
> *(…)"*[168]

---

[164] Mondelinge inlichtingen T-Mobile van 1 december 2011. T-Mobile inspecteert en analyseert voor dit doeleinde bijvoorbeeld de volgende gegevens: [VERTROUWELIJK].
[165] Idem, bijlage 4.
[166] Algemene Voorwaarden T-Mobile Netherlands B.V. abonnee consument (versies: geldig vanaf 31 mei en januari 2011) en Algemene Voorwaarden T-Mobile Abonnee Consument (geldig vanaf 10 mei 2010). Algemene Voorwaarden T-Mobile PrePaid (geldig vanaf oktober 2010).
[167] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, bijlage 4.
[168] T-Mobile Privacy Statement (versie april 2012).

Het nieuwste Privacy Statement (versie december 2012) van T-Mobile bepaalt, voor zover voor dit onderzoek van belang:

> *"(…) Om dit goed te kunnen doen houdt T-Mobile bij wat er gebeurt op haar netwerk. Hiervoor gebruiken we geavanceerde technieken die virussen kunnen herkennen, maar ook het gebruik van apps en toepassingen op ons netwerk en veelbezochte websites zien. Deze informatie kunnen wij gebruiken om (…) data te comprimeren (zoals streaming video) (…)."*[169]

[169] T-Mobile Privacy Statement (versie december 2012).

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).[170] 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 (hierna: e-Privacyrichtlijn) (geïmplementeerd in de Telecommunicatiewet; hierna: Tw).[171] De e-Privacyrichtlijn regelt de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor gebruikers van openbare elektronische communicatiediensten.[172] 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).[173] Er is geen sprake van een *lex specialis*-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene.[174] 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).[175]

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 van de Wbp. In de gevallen dat de specifieke wetgeving niet valt onder het bereik*

---

[170] *"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.

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

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

[173] 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."*

[174] 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).

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

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."[176]

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).

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*.[177]

[176] *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 concretiseringen 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).

[177] 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*

T-Mobile, gevestigd te Den Haag, Nederland, bepaalt de doeleinden van en de middelen voor de verwerking van persoonsgegevens bij de inzet van data-analysetechnieken op het dataverkeer over haar mobiele netwerk.[178] T-Mobile heeft zich, voor zover voor dit onderzoek van belang, op 22 februari 2010 als verantwoordelijke gemeld bij het CBP.[179] Uit de gegevens uit het Handelsregister volgt dat T-Mobile bevoegd is om doel en middelen vast te stellen. T-Mobile 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.[180]

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.*"

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*

---

voor de verwerking van de aanvullende persoonsgegevens die noodzakelijk zijn voor de werking van de dienst".

[178] Zie ook T-Mobile Privacy Statement (versie december 2012): *"T-Mobile Netherlands B.V. (Waldorpstraat 60, 2521 CC Den Haag) is verantwoordelijk voor de juiste verwerking van je gegevens."*

[179] Zie de meldingen met nummers m1070731 en m1070767 (versienummers 5.0).

[180] 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".*

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.[181]

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking[182] hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of - gezien de context[183] waarin ze worden verwerkt - medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.[184] 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.[185] 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.[186] Als voorbeeld wordt in de wetsgeschiedenis bij de Wbp genoemd het telefoonnummer.[187]

---

[181] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46.
[182] 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 (URL laatst bezocht op 29 mei 2013): *"Er is sprake van informatie "betreffende" een persoon wanneer het gaat om informatie "over" die persoon"*, met andere woorden, de inhoud. Idem, p. 11
[183] Vgl. idem: Er is sprake van informatie 'betreffende' een persoon *"wanneer, rekening houdende met alle omstandigheden van het precieze geval, gegevens worden gebruikt of waarschijnlijk zullen worden gebruikt met het doel een persoon te beoordelen, op een bepaalde wijze te behandelen of de status of het gedrag van die persoon te beïnvloeden"*, met andere woorden, het doel.
[184] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 46. Vgl. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 11: 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.
[185] *Kamerstukken II* 1997/98, 25 892, nr. 3, 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."*
[186] Idem, p 46-47.
[187] 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 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

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."*[188]

Een persoon is identificeerbaar indien zijn identiteit - direct of via nadere stappen, door gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor zijn persoon[189] - redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.[190] 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.[191] Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke. [192] In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.[193]

Beoordeling

Het CBP heeft in paragrafen 2.4 tot en met 2.6 (p. 22 e.v. van dit rapport) vastgesteld dat T-Mobile in verschillende apparatuur en systemen (onder andere afhankelijk van of zij die websites bezoeken of apps en protocollen gebruik(t)en) combinaties van de gegevens over en uit het dataverkeer van abonnees van haar dataverkeersdiensten (betrokkenen) verwerkt(e) als beschreven in **bijlage II** bij dit rapport.

Daarbij beschikt T-Mobile over de NAW-gegevens en/of e-mailadressen van (een groot deel van) haar abonnees, op grond van hun contractuele relatie.

Rb. Dordrecht 31 augustus 2004, *NBSTRAF* 2004, 422 over het GSM-nummer (MSISDN) als persoonsgegeven.

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

[189] 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.

[190] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip 'onevenredige inspanning' opgemerkt: *"Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen." Kamerstukken II* 1998/99, 25 892, nr. 13, p. 2.

[191] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48. Vgl. ook WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, 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. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 16.

[192] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48-49.

[193] Idem, p. 49. Registratiekamer 27 maart 1995, 95.V.029.

Het CBP heeft in paragrafen 2.4 tot en met 2.6 (p. 22 e.v. van dit rapport) vastgesteld dat T-Mobile de hierboven genoemde gegevens over en uit het dataverkeer verzamelt, gebruikt (en voor de doeleinden netwerkbeheer en -integriteit en troubleshooting vastlegt en bewaart op persoonsniveau, althans geaggregeerd per abonnee. Dit doet zij om het data ge-/verbruik en netwerkgebruik van betrokkenen in kaart te brengen.

Gegevens 'betreffende' een persoon
Het MSISDN, IMSI-klantnummer en het IMEI-toestelnummer (unieke klant- of toestel identifiers), op zichzelf of in onderlinge combinatie of in samenhang met (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over zijn mobiele data ge-/verbruik).[194] Datzelfde geldt voor de locatiegegevens ([VERTROUWELIJK]), 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. T-Mobile 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 (gedownloade) bestanden en verzonden en ontvangen e-mails op virus- en malware-herkenningspatronen om virussen/malware tegen te houden en te verwijderen of aan het analyseren 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 T-Mobile 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.[195]

Niet doorslaggevend is of T-Mobile 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 gebruikt[196], en die mogelijkheid is aanwezig. T-Mobile beschikt, zoals aangegeven, bijvoorbeeld over informatie over het mobiele datagebruik van individuele betrokkenen (het bezoek aan en gebruik van apps , websites en protocollen, frequentie en duur/tijd), data verbruiksgegevens (volume) en

[194] Hieruit volgt informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie.
[195] 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.cbpweb.nl/Pages/pv_20110913_google.aspx (URL laatst bezocht op 29 mei 2013).
[196] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.

contactgegevens (waaronder het MSISDN; unieke klantidentifier, e-mailadres(sen) en/of NAW-gegevens).

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 T-Mobile direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).

Postpaid abonnees
Ten aanzien van T-Mobile abonnees met een postpaid data abonnement, geldt het volgende.

Het MSISDN, het unieke IMSI-klantnummer[197] en het unieke IMEI-toestelnummer van een abonnee met een postpaid data abonnement zijn voor T-Mobile identificerend omdat zij een koppeling(smogelijkheid) heeft tussen deze nummers, gecombineerd met NAW-gegevens en/of e-mailadres(sen). Er kan dus een relatie tussen de gegevens worden gelegd.

T-Mobile beschikt verder over een koppeling(smogelijkheid) tussen de unieke klant- en/of toestel identifier(s) en (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen dan wel (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene.[198]

Niet alleen beschikt T-Mobile 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 het kopje 'Verloop onderzoek', p. 9 e.v. 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 T-Mobile moet verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is.

T-Mobile brengt in haar zienswijze 1 naar voren dat is voorzien in technische en organisatorische beveiligingsmaatregelen om een zorgvuldige en rechtmatige gegevensverwerking te waarborgen. Deze maatregelen betreffen een intern en extern (vanuit het moederbedrijf, en via onder andere externe audits) gehandhaafd beleid met betrekking tot functiescheidingen, beveiligingseisen, toegang tot applicaties en de verzamelde gegevens etc. Volgens T-Mobile wordt ook daarmee ervoor gezorgd dat de voor het netwerkbeheer vereiste gegevens beschikbaar zijn, alsmede dat deze

[197] Aan dit IMSI zijn alle gegevens van een abonnee gebonden, zoals NAW-gegevens, of de abonnee prepaid is of een abonnement heeft en of deze wel of niet in het buitenland mag bellen.
[198] Ook hier kan een relatie tussen de gegevens worden gelegd.

gegevens alleen voor dat doel kunnen worden gebruikt door degenen die de gegevens daarvoor nodig hebben.[199]

Ten aanzien van de door T-Mobile gehanteerde technische en organisatorische maatregelen, waaronder toegangsautorisaties, toegangsbeveiliging en controle daarop geldt dat dit bovenal een technische en organisatorische waarborg betreft ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp.[200] De omstandigheid dat slechts bepaalde medewerkers toegang hebben tot de data-analyse apparatuur en de data die met behulp daarvan wordt verwerkt, leidt echter niet tot de conclusie dat er geen sprake is van persoonsgegevens. De toegepaste aggregatie op abonnee-niveau (via de [VERTROUWELIJK: apparatuur]) is geen anonimisering[201] of gegevensvernietiging. De [VERTROUWELIJK] bevatten nog [VERTROUWELIJK] het e-mailadres van de T-Mobile abonnee die met een e-mailaccount van een (andere) provider mailt of een derde die een T-Mobile klant mailt).[202]

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

(i) netwerkbeheer en het waarborgen van netwerkintegriteit en -veiligheid, daaronder mede begrepen het voorkomen van congestie: om inzicht te hebben/krijgen in welke soorten diensten (apps/websites etc.) welke hoeveelheid capaciteit innemen op de verschillende delen van het netwerk en heavy users te identificeren;[203]
(ii) het oplossen van technische incidenten, en klantproblemen in individuele gevallen (troubleshooting);[204] en
(iii) optimalisatie van de dienstverlening aan klanten (waaronder videocompressie, afhankelijk van [VERTROUWELIJK] en van de door de gebruiker ingestelde setting).[205]

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

---

[199] Zienswijze 1 T-Mobile, p. 3.
[200] Naleving van het bepaalde in artikel 13 van de Wbp (beveiliging) valt buiten de scope van dit onderzoek.
[201] Anonimiseren wordt in de wetsgeschiedenis bij de Wbp gedefinieerd als *"een vorm van vernietigen van persoonsgegevens althans in de gevallen dat de verwijdering van de naam ook tot gevolg heeft dat de betrokkene niet meer kan worden herleid. Alleen in dit laatste geval pleegt te worden gesproken van «anonimiseren»." Kamerstukken II* 1999/2000, 25 892, nr. 92c, p. 13.
[202] Idem, Annex, p. 16 en [VERTROUWELIJK: apparatuur]. Vgl. ook [VERTROUWELIJK: apparatuur].
[203] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1. Zie ook reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2 en Zienswijze 1 T-Mobile, randnummer 6.
[204] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 1-2. Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 2. Idem, p. 4: *"Troubleshooting wordt gedaan op verzoek van dan wel in direct overleg met de klant voor het oplossen van een individueel probleem. Veelal wanneer de klant zelf aan de lijn is met onze klantenservice."*
[205] Brief T-Mobile van 19 september 2011, p. 2.

In de opinie van de Artikel 29 Werkgroep, het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders, over het begrip persoonsgegeven 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 informatie moet dan ook worden beschouwd als informatie betreffende identificeerbare personen, wat betekent dat voor de verwerking de regels inzake gegevensbescherming gelden."*[206] 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.[207]

Om de hiervoor genoemde doeleinden (i) tot en met (iii) te verwezenlijken moeten de verwerkte gegevens herleidbaar zijn tot de betrokken abonnees. De gegevensverwerking is (dan) mede gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

Prepaid abonnees

Ten aanzien van T-Mobile abonnees met een prepaid data abonnement geldt het volgende.

T-Mobile heeft verklaard dat zij NAW-gegevens en/of e-mailadressen heeft van [VERTROUWELIJK] van het totaal aantal prepaid abonnees ([VERTROUWELIJK]).[208]

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."*[209]

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

Ten aanzien van de prepaid abonnees van wie T-Mobile geen NAW-gegevens en/of e-mailadressen heeft, beschikt T-Mobile wel over ten minste MSISDN (een direct contactgegeven door middel waarvan T-Mobile met de abonnee in contact kan treden,

[206] WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 16-17.
[207] Idem, p. 22.
[208] Reactie T-Mobile op verzoek om inlichtingen van 11 april 2012, p. 1.
[209] *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 80.

om zijn identiteit vast te stellen), IMSI- en/of IMEI-nummer, en vaak ook locatiegegevens.

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 naam te achterhalen. De definitie van "persoonsgegeven" weerspiegelt ook dit feit"*, (onderstreping toegevoegd door het CBP).[210]

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."*[211]

Zakelijke abonnees

T-Mobile brengt in haar zienswijze 1 naar voren dat veel abonnees van T-Mobile ondernemingen en/of rechtspersonen zijn, en in de gevallen waarin deze zelf binnen de eigen organisatie zorgdragen voor de uitgifte van MSISDN's, SIM's etc. kunnen de betreffende eindgebruikers volgens T-Mobile niet worden geïdentificeerd, zodat geen sprake is van persoonsgegevens.[212]

Ook bedrijfsinformatie (bijvoorbeeld het 06-nummer en bedrijfs-e-mailadres van een zakelijke abonnee die normaliter wordt gebruikt door een specifieke werknemer) is in een aantal gevallen als persoonsgegeven te beschouwen, bijvoorbeeld omdat de naam van de werknemer binnen dat bedrijf wordt vastgelegd. Ook gegevens over eenmanszaken en bedrijven handelend onder een eigennaam worden als persoonsgegevens aangemerkt, wanneer die ook iets zeggen over het gedrag van de eigenaar.[213]

---

[210] WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 14-15.
[211] HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.
[212] Zienswijze 1 T-Mobile, p. 9.
[213] Vgl. 'Klant in het web. Privacywaarborgen voor internettoegang', A&V-studie nr. 17, Registratiekamer juni 2000, p. 34 en 58. URL: http://www.cbpweb.nl/downloads_av/av17.pdf (URL laatst bezocht op 29 mei 2013). 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*

Gelet op het voorgaande zijn de in deze paragraaf genoemde gegevens van T-Mobile abonnees met een (prepaid of postpaid) data abonnement persoonsgegevens 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.[214]

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*

---

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.

[214] Vgl. WP29 185, Opinion 13/2011 on Geolocation services on smart mobile devices van 16 mei 2011. URL: http://www.cbpweb.nl/downloads_int/wp185_en.pdf. Zie ook Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010 (z2010-00582), p. 34 e.v. 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://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf (URL's laatst bezocht op 29 mei 2013).

bij de traditionele spraaktelefonienetwerken. Dit is relevant voor de tenuitvoerlegging van de richtlijn."[215]
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 routering, 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 (…)"*[216]

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 verkeersgegevens zijn, is afhankelijk van het doel van de verwerking, te weten: voor het overbrengen van communicatie of voor andere doelen.[217]

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."*[218]

---

[215] 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.).
[216] 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.
[217] W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?', *Computerrecht* 2003, p. 28.
[218] *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 communicatie[219] 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 (hierna: Handvest).[220] Het Europees Hof voor de Rechten van de Mens (hierna: 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).[221]

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."*[222]

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

---

[219] *"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).

[220] 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.cbpweb.nl/Pages/adv_z2012-00746.aspx (URL laatst bezocht op 29 mei 2013).

[221] EHRM 3 april 2007, *NJ* 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44.

[222] *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 (…)."*

onderscheid tussen deze begrippen nog worden gemaakt langs de lijn van de 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 wetsgeschiedenis[223] geeft een indicatie welke categorieën van gegevens over en uit het dataverkeer als verkeersgegevens moeten worden aangemerkt. Beide noemen onder andere de routering, de duur, het tijdstip, het volume van de communicatie en het gebruikte protocol 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 URL en de hostname (URL op hoofddomein), 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.[224] De verkeersgegevens over het communicatiegedrag van betrokkenen (bijvoorbeeld URL's) zijn gegevens van gevoelige aard.[225] 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 websurfgedrag."*[226] En: *"Het gaat niet om het opslaan van websites die zijn bezocht."*[227] De

[223] 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.
[224] 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.
[225] *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.
[226] *Kamerstukken I* 2008/09, 31 145, C, p. 17. Zie in dezelfde zin idem, p. 12.

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 (hierna: 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 app-herkenning (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 een protocol. In deze initiatiefase vindt nog geen overbrenging plaats van communicatie.

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 packets al communicatiegegevens bevatten.

Omdat het niet mogelijk is om vooraf te bepalen wanneer de initiatiefase begint, zullen bij de data-analyse 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 worden beoordeeld als verkeersgegevens, tevens persoonsgegevens.

(Louter) gegevens uit het dataverkeer worden beoordeeld als communicatie tevens persoonsgegevens**.** Ten aanzien van virus- en malwareherkenningsgegevens uit (gedownloade) bestanden en verzonden en ontvangen e-mails geldt, voor zover T-Mobile deze verwerkt om 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).[228]

Samengevat, kunnen de persoonsgegevens worden ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het 06-nummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume, IP-adres van-naar met poortnummer/protocol, URL's, locatiegegevens etc.

[227] *Handelingen II* 2007/08, 83, p. 5836.
[228] Het CBP heeft bovenstaande toepassing van de begrippen "communicatie" en "verkeersgegevens" 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 deze begrippen in dit rapport.

2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk 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.[229] Ook het genereren van persoonsgegevens is een verwerking.[230] Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze gegevens.[231] 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).[232] Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen (*mere conduit*), verwerkt daarmee geen persoonsgegevens.[233]

Beoordeling

Het CBP heeft in paragraaf 3.5 (p. 56 e.v. van dit rapport) vastgesteld dat T-Mobile 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). T-Mobile verwerkt (aldus) persoonsgegevens die (in de meeste gevallen) ook verkeersgegevens zijn. Er is geen sprake van een mere conduit-uitzondering.

Ofwel T-Mobile verkrijgt (verzamelt) de persoonsgegevens via het gebruik van data-analysetechnieken. Zo inspecteert T-Mobile voor netwerkplanning- en beheer headergegevens in een datapakket dat van het toestel van de abonnee naar de applicatieserver gaat, (ii) voor virus- en malware bestrijding (gedownloade) bestanden en verzonden en ontvangen e-mails om virussen/malware tegen te houden en te verwijderen, (iii) voor troubleshooting het dataverkeer op bijvoorbeeld (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan

---

[229] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 51-52.
[230] Idem, p. 51
[231] 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.
[232] Met dien verstande dat de desbetreffende handelingen met betrekking tot verkeersgegevens van abonnees die geen natuurlijke personen zijn niet zonder meer persoonsgegevens zijn.
[233] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 68: *"Zodra er enige feitelijke macht over persoonsgegevens is, is het wetsvoorstel van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking kunnen onder de wettelijke regeling vallen. Cruciaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige) invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend. Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing"*, (onderstreping toegevoegd door het CBP). Idem, p. 51-52.

(ordening van al aanwezige gegevens) en (iv) voor videocompressie de URL van de website/video om de gebruikte service (flash video) te kunnen herkennen.[234] Ofwel T-Mobile analyseert/analyseerde via het gebruik van data-analysetechnieken persoonsgegevens die worden aangemaakt in haar mobiele netwerk (bijvoorbeeld dataverbruik gegevens om te kunnen factureren).

Gelet op het voorgaande verwerkt T-Mobile persoonsgegevens als bedoeld in artikel 1, aanhef en 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, eerste en tweede lid, 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.[235]

> 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 <u>en de daarmee verband houdende gegevens</u> 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*
> *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 afluisteren, aftappen,

[234] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 68.
[235] *Kamerstukken I* 2011/12, 32 549, E, p. 2.

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.

In de wetsgeschiedenis bij artikel 11.2a is opgemerkt over *Deep Packet Inspection*: *"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 afluisteren, 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).[236]

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 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."*[237]

[236] Idem, p. 13.
[237] *Kamerstukken I* 2011/12, 32 549, F, p. 5.

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."*[238]

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.
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:

[238] *Kamerstukken II* 2010/11, 32 549, nr. 16, p. 2-3.

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. (…)[239]
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.[240] Voor dataverkeer is dit bijvoorbeeld afhankelijk van het type dienst.[241]
Onder het begrip 'anonimiseren' wordt verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken.[242] 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.[243] 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:

---

[239] 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.
[240] *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 154.
[241] 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.
[242] *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 80.
[243] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48.

> *"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).[244] 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."*[245]

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).[246] Het gaat hier niet om zelfstandige verwerkingsdoelen, maar om verwerkingsdoelen die van het factureringsdoel en het overbrengen van de communicatie zijn afgeleid.[247] 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" (…)."*[248]

---

[244] *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 155.
[245] Idem, nr. 13, p. 20.
[246] Idem, nr. 3, p. 156.
[247] Idem.
[248] EHRM 25 maart 1983, nr. 97 (Silver & Others v. United Kingdom).

Het Hof van Justitie van de EG vult het begrip noodzakelijkheid, 'een autonoom begrip van gemeenschapsrecht', op een strikte wijze in.[249] 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.[250]

Ten aanzien van de verwerking ten behoeve van de facturering geldt dat het noodzakelijkheidscriterium 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.[251] 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.[252]

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 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).[253]

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."* [254]

---

[249] Vgl. ook HvJ EG 16 december 2008, *EHRC* 2009, 23 (*LJN* BG7811; Huber), r.o. 52.
[250] 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.*"
[251] 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).
[252] Idem.
[253] 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.
[254] *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 54. Zie ook *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 6.

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.[255]

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.[256] 'Specifiek' betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).[257] 'Geïnformeerd' betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.[258]

Van *ondubbelzinnige* toestemming is slechts sprake indien bij de verantwoordelijke elke twijfel is uitgesloten over de vraag of de betrokkene zijn toestemming heeft

[255] 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.
[256] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.
[257] 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/files/2011/wp187_nl.pdf (URL laatst bezocht op 29 mei 2013).
[258] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.

gegeven.[259] '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).[260] 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."*[261]

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."[262]

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.[263] Daarbij geldt als voorwaarde dat het moet gaan om een overeenkomst waarbij de betrokkene partij is[264] en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (dat wil zeggen: als de overeenkomst niet goed kan worden uitgevoerd zonder de persoonsgegevens).[265]

De uitgever van een krant mag bijvoorbeeld de persoonsgegevens van zijn abonnees verwerken omdat dat noodzakelijk is om de krant te kunnen bezorgen[266] (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

---

[259] Idem, p. 80.
[260] 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.
[261] *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.
[262] WP29 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 41.
[263] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80.
[264] 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.
[265] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 81.
[266] *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 (URL laatst bezocht op 29 mei 2013).

niet echt noodzakelijk is aangezien er een manier bestaat om de overeenkomst uit te voeren zonder de persoonsgegevens (proportionaliteits- en subsidiariteitstoets).[267] 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*.[268] 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.[269] Daarbij geldt als voorwaarde dat het moet gaan om een verplichting, opgenomen in een wettelijke bepaling, die op de verantwoordelijke rust en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (zonder verwerking van de persoonsgegevens moet het uitvoeren van de wettelijke verplichting redelijkerwijs niet goed mogelijk zijn; proportionaliteits- en subsidiariteitstoets).[270] Anders gezegd: er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.[271] Daarbij moet onder andere worden gelet op de aard van de in het geding zijnde taak en de aard van de betrokken persoonsgegevens.[272] 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. [273] 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.[274]

---

[267] 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).

[268] 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."*

[269] 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.

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

[271] Idem, p. 82.

[272] Idem, p. 83.

[273] Idem.

[274] Idem.

Gerechtvaardigd belang

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

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke (bijvoorbeeld om zijn reguliere bedrijfsactiviteiten te kunnen verrichten[275]) 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).[276]

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.[277] 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.[278]

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 persoonsgegeven mogen worden verwerkt. Artikel 8 omvat derhalve een uitputtende opsomming van verwerkingsgronden."*[279]

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 (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).[280]

---

[275] Idem, p. 86.
[276] 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.
[277] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 87.
[278] Idem.
[279] *Kamerstukken II* 1998/99, 25 892, nr. 13, p. 5-6.
[280] Onder 'overbrenging van communicatie' en 'facturering' moet ook verkeersbeheer, behandeling van verzoeken om inlichtingen van abonnees en opsporing van fraude

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp[281] 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).[282] 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).[283] 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) verwerkingsdoelen, 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 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. Materieel (inhoudelijk) betekent 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.

---

worden begrepen (artikel 11.5, vijfde lid, van de Tw). De verkeersgegevens mogen (ook) voor die (afgeleide) verwerkingsdoelen worden verwerkt, voor zover noodzakelijk.

[281] 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 verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

[282] *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.

[283] 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.

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.[284] Het artikel geeft (dus) geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

Als hoofdregel geldt zoals vermeld op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het afluisteren, 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 waarborgen van de integriteit en de veiligheid van 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) doelen, 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)[285] 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 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. Materieel (inhoudelijk) betekent 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

[284] 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.

[285] 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*).

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 Netwerkbeheer en -integriteit

Netwerkplanning en -beheer

[VERTROUWELIJK]
Het CBP heeft in paragraaf 2.4, onder het kopje 'A. Netwerkplanning en -beheer' (p. 26e.v. van dit rapport) vastgesteld dat T-Mobile wat betreft één specifieke gegevensverwerking via de [VERTROUWELIJK: apparatuur] met betrekking tot websitegebruik en app- en protocolgebruik gegevens inspecteert/genereert, gebruikt, vastlegt en gedurende 14 dagen bewaart voor netwerkplanning en -beheer. Het CBP heeft tevens vastgesteld dat T-Mobile het 06-nummer direct na het verzamelen verwijdert, maar dat deze gegevens nog wel [VERTROUWELIJK] het e-mailadres van de T-Mobile abonnee die met een e-mailaccount van een (andere) provider mailt of een derde die een T-Mobile klant mailt) kunnen bevatten.

Wat betreft een andere gegevensverwerking via de [VERTROUWELIJK: apparatuur] met betrekking tot hoogverbruik van data inspecteert/genereert, gebruikt, legt vast en bewaart T-Mobile gedurende 45 dagen 06-nummer met het verbruikte datavolume van zogeheten heavy users.

Het CBP heeft in paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Ten aanzien van de gegevensverwerking met betrekking tot websitegebruik en app- en protocolgebruik, geldt het volgende.

T-Mobile stelt in haar zienswijze 1 dat de in het rapport beoordeelde gegevensverwerkingen internetverkeersgegevens betreffen, waarop allereerst artikel 11.5 van de Tw van toepassing is. Voor zover er sprake is van de verwerking van persoonsgegevens kunnen volgens T-Mobile verschillende van de in artikel 8 van de Wbp opgesomde grondslagen daaraan ten grondslag worden gelegd (artikel 8, aanhef en onder b, c en f).[286] T-Mobile voegde daar in haar zienswijze 1 aan toe dat een en ander wordt ingevuld door in de Tw opgenomen nieuwe bepalingen, waaronder artikel 11.2a van de Tw.[287]

[286] Zie o.a. Zienswijze 1 T-Mobile, p. 8-9.
[287] Idem, 8: "*Uit artikel 11.5, eerste en tweede lid, Tw volgt dat verkeersgegevens mogen worden verwerkt voor het overbrengen van de communicatie en de facturering daarvan. Uit het vijfde lid van het artikel volgt dat onder deze doeleinden mede wordt begrepen het verkeersbeheer, de behandelingen van verzoeken om inlichtingen van klanten, alsmede de opsporing van fraude. (…) Een en ander wordt ingevuld door twee binnenkort in de telecommunicatiewet op te nemen nieuwe bepalingen, zijnde artikel 7.4a Tw en artikel 11.2a Tw. Daaruit kan worden opgemaakt dat het telecomaanbieders in elk geval is toegestaan om het gegevensverkeer over hun netwerken te analyseren, voor zover dat nodig is ter waarborging van de integriteit en veiligheid van hun netwerken en/of voor zover dat nodig is ter uitvoering van een wettelijk voorschrift of rechterlijk beve.*"

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 afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie én 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. 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 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-analysetechnieken 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 (mits er een proportionele implementatie is).[288]

Ten aanzien van het inspecteren/genereren (verzamelen) van de persoonsgegevens geldt dat er voor T-Mobile een noodzaak was om de gegevens op deze niet-geanonimiseerde wijze te verwerken om de benodigde informatie te hebben/(kunnen) krijgen over de netwerkbelasting als gevolg van (de toename van) het gebruik van allerlei apps en websites. T-Mobile 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 persoonsniveau te gebruiken, vast te leggen en te bewaren. Getoetst moet worden of ook die 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-analysetechnieken naar aanleiding van het

[288] 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.

gebruik van het netwerk van de aanbieder) 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 in de belangenafweging. Daarnaast worden de inspanning en kosten meegewogen die voor T-Mobile gepaard gaan met de ontwikkeling en implementatie van 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.

In algemene zin geldt dat het herkennen/identificeren van het bezoek aan en gebruik van apps, websites en protocollen 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 en protocollen 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 groot zijn.

Daarbij leert de praktijk dat ondanks (passende) technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, (beveiligings)incidenten niet altijd kunnen worden voorkomen. Gelet op de aard van de verzamelde gegevens bieden andere maatregelen dan het zo snel als mogelijk 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.

T-Mobile heeft aannemelijk gemaakt dat zij voor netwerkplanning en -beheer trends en ontwikkelingen die (verwacht worden) zich voor (te) doen, en die aanleiding kunnen zijn om de netwerkcapaciteit aan te passen, moeten kunnen herkennen.[289] *O*m zulke trends te berekenen is statistische analyse nodig.

Het CBP oordeelt dat om zulke trends in gebruikersverkeer te identificeren voor netwerkplanning en -beheer de persoonsgegevens (daarom) kunnen worden geaggregeerd naar gebruikersgroepniveau 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

[289] Reactie T-Mobile op vordering van 21 februari 2013, p. 4 Zie ook idem, p. 5 over het gebruik van data-analyse oplossingen: *"De gegevens over en/of uit het mobiele dataverkeer van individuele klanten worden door T-Mobile en met behulp van haar huidige data-analyse oplossingen onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen geanonimiseerd of zodanig geaggregeerd dat deze niet met individuele klanten in verband kunnen worden gebracht."*

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 wijst - nu de door T-Mobile voor netwerkplanning verwerkte gegevens in feite worden gebruikt voor kwantitatief statistisch onderzoek verder op 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.[290]

T-Mobile heeft verklaard dat [VERTROUWELIJK].[291] Dit vormt een implementatie van een zogeheten privacy filter om de gegevens zo snel als mogelijk na het verzamelen onomkeerbaar te anonimiseren. Een privacy filter is een van de technische mogelijkheden om het aantal persoonsgegevens tot het strikt noodzakelijke minimum te beperken.[292]

Ofschoon T-Mobile (aldus) het 06-nummer zo snel als mogelijk verwijdert, kunnen de geaggregeerde data evenwel nog wel e-mailadressen bevatten, te weten: in het geval een T-Mobile abonnee met een e-mail account van een (andere) provider mailt of een derde een T-Mobile klant mailt). Dit terwijl ook op het punt van de e-mailadressen de persoonsidentificerende kenmerken direct na het verzamelen op eenzelfde wijze kunnen worden verwijderd.

Het CBP neemt vervolgens de consequenties in aanmerking voor de continuïteit en integriteit van haar netwerk als T-Mobile 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 T-Mobile bij de implementatie van een alternatieve oplossing.

T-Mobile heeft in haar zienswijze 2 - weliswaar - genoemd dat alleen al de kosten van de *vervanging* van de in gebruik zijnde [VERTROUWELIJK]-apparatuur door andere (T-Mobile niet bekende of beschikbare) apparatuur moet worden [VERTROUWELIJK].[293] T-Mobile heeft ondanks de vordering van het CBP daartoe geen inschatting gegeven van de kosten (in euro's) en de tijd die het kost (in kalenderdagen) om voor het 'subdoeleinde' van verkeersbeheer (een) data-analyse oplossing(e) te (laten) ontwikkelen, implementeren en beheren die T-Mobile in staat zou stellen om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen te anonimiseren of zodanig te aggregeren dat deze niet met individuele klanten in verband kunnen worden gebracht dan wel om de

[290] HvJ EG 16 december 2008, *EHRC* 2009, 23 (*LJN* BG7811; Huber).
[291] Zienswijze T-Mobile van 12 februari 2012, p. 14 en 16 en Zienswijze 2 T-Mobile, p. 14.
[292] Andere technische mogelijkheiden zijn bijvoorbeeld: (i) het (laten) aanpassen van configuratie-instellingen op bestaande data-analyse apparatuur, zodat de gegevens/persoonsidentificerende kenmerken zo snel als mogelijk na het verzamelen worden verwijderd uit de verkregen dataset, (ii) het (doen) vervangen van bestaande data-analyse apparatuur door apparatuur die (wel) in staat is om de gegevens zo snel als mogelijk na het verzamelen onomkeerbaar te anonimiseren (in niet-persistent (werk)geheugen) enz.
[293] Zienswijze 2 T-Mobile, p. 14.

verwerking van niet-geanonimiseerde gegevens te beperken tot die klanten die daarvoor hun (ondubbelzinnige) toestemming hebben gegeven.

Het CBP neemt als het gaat om het maken van kosten door T-Mobile ook mee in zijn beoordeling dat T-Mobile mogelijk een beroep kan doen op de garantie in de contractsdocumentatie van de [VERTROUWELIJK: apparatuur] dat de producten en diensten voldoen aan de geldende wettelijke normen.[294]

Anderzijds betrekt het CBP in zijn beoordeling het risico voor de betrokkenen van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, gelet op de bewaartermijn.

Het CBP oordeelt dat omdat T-Mobile eventuele e-mailadressen niet zo snel mogelijk verwijdert, terwijl dat wel mogelijk is en was, het gedurende 14 dagen bewaren en verwerken van de gegevens in niet-geanonimiseerde vorm toch niet als noodzakelijk kan worden beschouwd. T-Mobile heeft immers ook technische maatregelen kunnen nemen om [VERTROUWELIJK] voor websitebezoek en app- en protocolgebruik het MSISDN direct na het verzamelen, te verwijderen.

Ten aanzien van de gegevensverwerking met betrekking tot hoogverbruik van data, geldt het volgende.

Bij [VERTROUWELIJK] het verbruikte datavolume per top subscriber (heavy user abonnee) - wordt het MSISDN *niet* door T-Mobile verwijderd. T-Mobile stelt dat deze gegevens noodzakelijk zijn om grootgebruikers te kunnen identificeren in het kader van de continuïteit en kwaliteit van het netwerk van T-Mobile.[295]

Het CBP neemt in aanmerking dat T-Mobile [VERTROUWELIJK] waarmee deze gegevens worden geabstraheerd ook gebruikt voor handhaving van de Fair Use Policy.[296] Gelet hierop valt niet in te zien wat het in niet-geanonimiseerde vorm zo lang verwerken nog toevoegt aan het gewenste resultaat. Voor het doel(einde) van netwerkcontinuïteit kan worden volstaan met statistische gegevens.

Omdat T-Mobile voor netwerkplanning en -beheer wat betreft deze andere gegevensverwerking met betrekking tot hoogverbruik van data het verzamelde 06-nummer niet zo snel mogelijk verwijdert, terwijl dat wel mogelijk is en was, kan het gedurende 45 dagen bewaren en verwerken van de gegevens in niet-geanonimiseerde vorm eveneens niet als noodzakelijk worden beschouwd.

Doordat de verwerking niet proportioneel en niet subsidiair is voor verkeersbeheer en omdat T-Mobile ook geen ander noodzakelijk verwerkingsdoel heeft voor de onder dit kopje besproken gegevensverwerking, handelt T-Mobile in strijd met artikel 11.5 van de Tw. Hierdoor kan van een grondslag als genoemd in artikel 8 van de Wbp evenmin sprake zijn en handelt T-Mobile tevens in strijd met artikel 8 van de Wbp.

---

[294] [VERTROUWELIJK]
[295] Zienswijze 1 T-Mobile, Annex, p. 16.
[296] Of T-Mobile een grondslag heeft voor de inzet van data-analyse technieken ten behoeve van (handhaving van) de fair use policy is niet door het CBP beoordeeld.

Virus- en malwarebestrijding
Het CBP heeft in paragraaf 2.4, onder het kopje 'B. Ongewenst dataverkeer' (p. 28 e.v. van dit rapport) vastgesteld dat T-Mobile (een) unieke klant- en/of toestelidentifier(s) in combinatie met virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer van betrokkenen genereert/verzamelt en gebruikt voor het (veilig) leveren van mobiel dataverkeer.

Het CBP heeft in paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook communicatie betreffen.

T-Mobile 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).

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, wordt onder andere begrepen het aanbieden van virusfilters voor inkomende en eventueel uitgaande e-mails en het bestrijden van spyware.

Het CBP heeft in paragraaf 2.4 (p. 28 van dit rapport) vastgesteld dat internet aanbieders ook naar de inhoud van (gedownloade) bestanden en verzonden en ontvangen e-mails moeten kijken virussen/malware te kunnen herkennen. Een alternatieve vorm van data-analyse waarbij bijvoorbeeld alleen naar headergegevens wordt gekeken, schiet tekort. Hieruit volgt dat de verwerking van de virus- en malwareherkenningsgegevens noodzakelijk is voor (de uitvoering van) de zorgplicht internetveiligheid.

Uit het voorgaande blijkt dat T-Mobile 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.

Oplossen en voorkomen van netwerkproblemen

[VERTROUWELIJK]
Het CBP heeft in paragraaf 2.4, onder het kopje '[VERTROUWELIJK: apparatuur]' (p. 32 e.v. van dit rapport) vastgesteld dat T-Mobile unieke klant- en toestelidentifiers in combinatie met (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan (gegevens zoals datavolume, [VERTROUWELIJK] en al dan niet geslaagde connecties) inspecteerde/genereerde, gebruikte, vastlegde en op verschillende aggregatieniveaus (vijftien minuten-, dag-, week- en maandbasis) gedurende respectievelijk dertig dagen, veertig dagen, één jaar en twee jaar bewaarde, voor het oplossen en voorkomen van netwerkproblemen.

Het CBP heeft in paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

T-Mobile stelt in haar zienswijze 1 dat de in het rapport beoordeelde gegevensverwerkingen internetverkeersgegevens betreffen, waarop allereerst artikel 11.5 van de Tw van toepassing is. Voor zover er sprake is van de verwerking van persoonsgegevens kunnen volgens T-Mobile verschillende van de in artikel 8 van de Wbp opgesomde grondslagen daaraan ten grondslag worden gelegd (artikel 8, aanhef en onder b, c en f).[297]

Ten aanzien van het inspecteren/genereren (verzamelen) van de persoonsgegevens geldt dat er voor T-Mobile een noodzaak was om de gegevens op deze niet-geanonimiseerde wijze te verwerken om de benodigde informatie te hebben/(kunnen) krijgen over het functioneren van het netwerk/toestel bij het gebruik daarvan. T-Mobile 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 persoonsniveau te gebruiken, vast te leggen en te bewaren. Getoetst moet worden of ook die 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-analysetechnieken naar aanleiding van het gebruik van het netwerk van de aanbieder) 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 in de belangenafweging. Daarnaast worden de inspanning en kosten die voor T-Mobile gepaard gaan met de ontwikkeling en implementatie van een alternatieve oplossing meegewogen, evenals de consequenties voor de continuïteit en integriteit van haar netwerk.

Het CBP begrijpt dat het voor de netwerkmonitoring van T-Mobile handig kan zijn om de gegevens zo lang in niet-geanonimiseerde vorm te verwerken, maar daarmee is

[297] Zie o.a. Zienswijze 1 T-Mobile, p. 8-9.

de gegevensverwerking niet automatisch ook noodzakelijk en daarmee gerechtvaardigd.

T-Mobile stelt zich meer in algemene zin op het standpunt dat het voor het oplossen en voorkomen van netwerkproblemen noodzakelijk is om gegevens op individueel niveau te verwerken. T-Mobile heeft dit in haar zienswijzen (nader) toegelicht aan de hand van [VERTROUWELIJK], daarvoor niet kan worden volstaan met de verwerking van geanonimiseerde gegevens.[298]

Het CBP neemt in aanmerking dat dit voorbeeld een situatie representeert waarin T-Mobile vooral op relatief korte termijn actie zal (moeten kunnen) ondernemen: het monitoren van incidenten en het managen daarvan.

Gelet op het voorgaande valt niet in te zien - en heeft T-Mobile onvoldoende aangevoerd om te oordelen - dat de bewaartermijnen op verschillende aggregatieniveaus (vijftien minuten-, dag-, week- en maandbasis) van respectievelijk dertig dagen, veertig dagen, één jaar en twee jaar noodzakelijk zijn. Het zolang verwerken van deze gegevens in niet-geanonimiseerde vorm voor deze doelstellingen is dus niet proportioneel.

T-Mobile heeft de bewaartermijnen van de persoonsgegevens wat betreft de verschillende aggregatieniveaus naar aanleiding van het onderzoek ook teruggebracht naar respectievelijk twee dagen, twee weken, tien weken en zes maanden (zie het kopje 'Getroffen maatregelen' hieronder).[299]

Omdat T-Mobile voor het oplossen en voorkomen van netwerkproblemen de persoonsgegevens die ook verkeersgegevens zijn niet zo snel als mogelijk 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 niet subsidiair was voor verkeersbeheer en omdat T-Mobile ook geen ander noodzakelijk verwerkingsdoel had voor de onder dit kopje besproken gegevensverwerking, handelde T-Mobile 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 T-Mobile tevens in strijd met artikel 8 van de Wbp.

Getroffen maatregelen

T-Mobile heeft de bewaartermijnen van de persoonsgegevens die ook verkeersgegevens zijn wat betreft de verschillende aggregatieniveaus verkort tot respectievelijk vijftien, vijftien en veertien dagen (zie paragraaf 2.4, p. 31 van dit rapport, onder het kopje 'Getroffen maatregelen').[300]

---

[298] Zie Zienswijze 2 T-Mobile, p. 4 en de Annex bij deze zienswijze en Zienswijze T-Mobile van 12 februari 2012, p. 7. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 7.

[299] Reactie T-Mobile op vordering van 21 februari 2013, p. 7: *"In het kader van het voortdurend streven naar verbetering van de periodieke controles van haar processen en procedures, heeft T-Mobile, zonder aanvaarding van enige gehoudenheid daartoe, de bovengenoemde bewaartermijnen en aggregatieniveaus inmiddels aangepast."*

[300] Het CBP leidt uit de reactie van T-Mobile op de vordering af dat er geen op maandbasis geaggregeerde data meer wordt bewaard. Reactie T-Mobile op vordering van 21 februari 2013, p. 7-8.

Het CBP oordeelt dat T-Mobile aannemelijk heeft gemaakt dat de inzet van de [VERTROUWELIJK: apparatuur] in deze nieuwe configuratie noodzakelijk is voor de stabiliteit en integriteit van het netwerk.

Doordat T-Mobile voor het oplossen en voorkomen van netwerkproblemen via de [VERTROUWELIJK: apparatuur] de persoonsgegevens inmiddels zo snel als mogelijk na het verzamelen verwijdert, heeft zij in zoverre wel een grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Op deze punten handelt T-Mobile niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

3.6.2 Troubleshooting

Het CBP heeft in paragraaf 2.5 (p. 37 e.v. van dit rapport) vastgesteld dat T-Mobile gegevens over het dataverkeer van betrokkenen[301] verzamelt, gebruikt en vastlegt om in specifieke, individuele gevallen inlichtingen te kunnen geven bij storingen en fouten.

Het CBP heeft in paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat dit een verwerking van persoonsgegevens tevens verkeersgegevens is.

T-Mobile heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming (artikel 8, aanhef en onder a, van de Wbp).[302] T-Mobile verwijst daarbij onder andere naar haar oude Privacy Statement (algemene voorwaarden).[303]

Ten aanzien van (de toets van) het verwerkingsdoel behandeling van verzoeken om inlichtingen van klanten als bedoeld in artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw, geldt het volgende.

T-Mobile heeft als verzamel- en verwerkingsdoeleinde van de persoonsgegevens genoemd 'het oplossen van technische incidenten, en klantproblemen in individuele gevallen (troubleshooting)'. Uit het voorgaande blijkt dat T-Mobile (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 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). Dit omdat 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.

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.

---

[301] Bijvoorbeeld, voor zover de gegevens binnen de scope van dit onderzoek vallen: (een) unieke klantidentifier(s) en [VERTROUWELIJK].
[302] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 4.
[303] Privacy Statement April 2011.

Indien en voor zover T-Mobile claimt dat ondubbelzinnige toestemming is/wordt verkregen via het Privacy Statement, wijst het CBP er - ten overvloede - op 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. 64 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."*[304] Hieruit volgt dat ondubbelzinnige toestemming niet via het Privacy Statement kan worden verkregen.

3.6.3 Videocompressie

Het CBP heeft in paragraaf 2.6 (p. 39 e.v. van dit rapport) vastgesteld dat T-Mobile gegevens over het dataverkeer van betrokkenen[305] genereert/verzamelt, en gebruikt voor video-optimalisatie.

Het CBP heeft in paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

T-Mobile heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming (artikel 8, aanhef en onder a, van de Wbp).[306] T-Mobile heeft nader toegelicht: *"Klanten [VERTROUWELIJK] kunnen desgewenst een andere setting kiezen via speed.t-mobile.nl (…)"*, (onderstreping toegevoegd door het CBP).[307]

Op grond van artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw is de verwerking van niet-geanonimiseerde verkeersgegevens toelaatbaar indien deze noodzakelijk is voor het verwerkingsdoel 'verkeersbeheer' (oftewel, activiteiten ter verbetering van de netwerk performance of de dienstverlening van de mobiele aanbieder). T-Mobile heeft aannemelijk gemaakt dat de verwerking van persoonsgegevens noodzakelijk is om bijvoorbeeld om bijvoorbeeld haar reguliere bedrijfsactiviteiten te kunnen verrichten, om de gewenste snelheid tot YouTube te garanderen of (zonder congestie) toegang te blijven faciliteren tot die website/app. Uit het voorgaande blijkt dat T-Mobile een beroep kan doen op het verwerkingsdoel verkeersbeheer (artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw). Zo'n verwerkingsdoel correspondeert met de grondslagen uitvoering van een overeenkomst en/of een noodzaak (artikel 8, aanhef en onder b en/of f, van de Wbp).

[304] *Handelingen I* 1999/2000, 34, p. 1632.
[305] Te weten: [VERTROUWELIJK]
[306] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 5.
[307] Bijlage 4 bij reactie T-Mobile op verzoek om inlichtingen van 8 september 2011.

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

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.[308]

'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).[309] Het doeleinde mag ook niet in de loop van het verzamelproces worden geformuleerd.[310] '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.[311]

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.*"[312]

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 paragraaf 3.3 (p. 44 e.v. van dit rapport) vastgesteld dat T-Mobile persoonsgegevens verzamelt/verwerkt bij de inzet van data-analysetechnieken in haar mobiele netwerk.

[308] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 79.
[309] Idem.
[310] Idem.
[311] Idem.
[312] Idem.

Uitdrukkelijk omschreven
T-Mobile heeft als doeleinden van de gegevensverwerking (samenvat weergegeven) geformuleerd, voor zover deze binnen de scope van dit onderzoek vallen: netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie). Deze doeleinden waren onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving in de meldingen die T-Mobile heeft gedaan. De melding dat gegevens worden verwerkt voor de doeleinden 'het registreren van gegevens over afgewikkeld verkeer van spraak en data ten behoeve van onderzoek naar hoogverbruik en (intern) fraudeonderzoek', 'het sluiten en uitvoeren van de overeenkomst die het gevolg is van een aansluiting' respectievelijk 'het analyseren van het gebruik van het netwerk' is onvolledig en onvoldoende duidelijk. Het biedt bijvoorbeeld onvoldoende houvast om te kunnen voorzien dat T-Mobile onder andere 'bijhoudt' welke apps, websites en toepassingen haar klanten gebruiken, zodat zij extra capaciteit in kan zetten als dat nodig is, alsmede analyseert welk toestel de betrokkene gebruikt en hoe dit toestel in haar netwerk functioneert, zoals het aantal succesvol opgezette verbindingen.[313] De afweging van de belangen van de verantwoordelijke en de betrokkene is zodoende onvoldoende controleerbaar.[314]

Het CBP heeft in paragraaf 2.1 (p. 15 van dit rapport) vastgesteld dat T-Mobile geen andere meldingen had gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analysetechnieken 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.[315] De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding.[316] T-Mobile heeft geen functionaris gegevensbescherming

[313] Vgl. Privacy Statement T-Mobile (december 2012).
[314] Idem, p. 132-133: *"Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn."*
[315] De enige artikelen die mogelijkerwijs in aanmerking zouden kunnen komen qua categorie(ën) 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.
[316] 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."*

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).

Ten aanzien van de stelling van T-Mobile in haar zienswijze 1 dat, voor zover voor dit onderzoek van belang, bijvoorbeeld uit haar Privacy Statement en de overeenkomsten met abonnees voldoende bleek dat zij persoonsgegevens verwerkt om haar diensten te verlenen en om de kwaliteit daarvan te waarborgen[317], neemt het CBP in aanmerking dat ofschoon blijkens de wetsgeschiedenis bij de vorm van de doelomschrijving lijkt te zijn gedacht aan de melding die zij op grond van artikel 27 jo. 28 van de Wbp (hierna: de meldingsplicht) verplicht is te doen[318], de recente opinie van de Artikel 29-werkgroep over doelbinding ook ruimte laat voor de vorm van verwoording en uitdrukking van de doeleinden in een privacystatement ('notice'): *"Expressing the purposes under the meaning of Article 6(1)(b) may be accomplished in different ways. These include, for example, describing the purposes in a notice provided to the data subjects, in a notification provided to the supervisory authority, or internally in the information provided to a data protection officer. Some national laws specifically provide that both notices and notifications are acceptable forms of complying with the requirement of making the purposes of the processing explicit, but that they are not the only possibilities"*, (onderstreping toegevoegd door het CBP).[319]

In het oude Privacy Statement van T-Mobile werd over de kwaliteit van de dienstverlening opgemerkt, voor zover voor dit onderzoek van belang: *"T-Mobile bewaakt de continuïteit van haar mobiele netwerk. T-Mobile monitoort daarvoor niet jouw individuele gebruik van het netwerk maar onderzoekt wel of er bijvoorbeeld ergens in het netwerk van T-Mobile problemen voorkomen, bijvoorbeeld storingen of piekverbruik"*, (onderstreping toegevoegd door het CBP).[320] De zinsnede in het oude Privacy Statement 'T-Mobile monitoort daarvoor niet jouw individuele gebruik van het netwerk' moet als feitelijk onjuist worden aangemerkt, althans is onvolledig en onvoldoende duidelijk. Verder kan T-Mobile niet volstaan met de mededeling dat gegevens (in abstracto) worden verwerkt om de kwaliteit van de dienstverlening te waarborgen: dit is te weinig specifiek.

De doeleinden van de gegevensverwerking netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie) waren aldus ook onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving in het oude Privacy Statement.

---

[317] Zienswijze 1 T-Mobile, p. 11.
[318] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 20 en 79: *"De omschrijving van het doel zal hetzij blijken uit de melding van de verwerking die de verantwoordelijke op grond van de wet uit hoofde van de wet verplicht is te verrichten – zie artikel 28, eerste lid, onder b, van het wetsvoorstel – hetzij uit de algemene maatregel van bestuur waarin precies zal worden geregeld welke verwerkingen van de meldingsverplichting worden vrijgesteld"* en *"Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen."*
[319] WP29 203. Opinion 03/2013 on purpose limitation van 2 april 2013, p. 18. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (URL laatst bezocht op 29 mei 2013).
[320] Privacy Statement April 2011.

Doordat T-Mobile de hiervoor genoemde doeleinden waarvoor zij persoonsgegevens verwerkt bij aanvang van het onderzoek onvolledig en onvoldoende duidelijk had omschreven bij haar meldingen/in haar oude Privacy Statement, werden de door T-Mobile verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelde T-Mobile in strijd met artikel 7 van de Wbp.

Gerechtvaardigd doeleinde
Het CBP heeft in paragraaf 3.6 (p. 58 e.v. van dit rapport) vastgesteld dat T-Mobile bij aanvang van het onderzoek niet in alle stadia van de verwerking een grondslag had voor de gegevensverwerkingen voor het doeleinde netwerkbeheer en –integriteit (meer in het bijzonder: netwerkplanning en -beheer en het oplossen en voorkomen van netwerkproblemen).

Doordat de gegevensverwerking voor het doeleinde netwerkbeheer en –integriteit 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 T-Mobile verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelde T-Mobile in strijd met artikel 7 van de Wbp.

Getroffen maatregelen
T-Mobile heeft haar meldingen eind 2011 (versie 6.0) en - wat betreft de melding met nummer m1070731 - per eind oktober 2012 (nogmaals) gewijzigd.

Uit het voorgaande (zie p. 17-18 van dit rapport) blijkt dat de doeleinden netwerkbeheer en -integriteit en troubleshooting (eerst) zijn omschreven bij de gewijzigde meldingen die T-Mobile heeft gedaan eind 2011 en dat het doeleinde optimalisatie van de dienstverlening aan klanten (waaronder begrepen videcompressie) alsnog is omschreven in de melding met nummer m10700731 per eind oktober 2012.

Doordat de doeleinden van de gegevensverwerking netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie) duidelijk zijn omschreven in de doelomschrijving in de gewijzigde meldingen, worden de door T-Mobile verzamelde persoonsgegevens inmiddels voor uitdrukkelijk omschreven doeleinden verzameld en handelt T-Mobile ten aanzien van het element ‘uitdrukkelijk omschreven’ niet langer in strijd met artikel 7 van de Wbp.

Doordat T-Mobile voor het oplossen en voorkomen van netwerkproblemen via de [VERTROUWELIJK: apparatuur] de persoonsgegevens gelet op de verkorting van de bewaartermijnen van de persoonsgegevens inmiddels zo snel als mogelijk na het verzamelen verwijdert, heeft zij in dit verband in zoverre een grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit. Hierdoor worden de door T-Mobile verzamelde persoonsgegevens op dit punt inmiddels voor een voor gerechtvaardigd doeleinde verzameld. De verwerking zonder grondslag én het verzamelen van persoonsgegevens zonder gerechtvaardigd doeleinde duurt voort voor de gegevensverwerking voor netwerkplanning en -beheer via de [VERTROUWELIJK: apparatuur].

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.[321]

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
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.[322]

Deze bepaling vormt een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing'.[323] 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.[324] 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.[325]

---

[321] Aanvullend bepaalt artikel 11.2a, derde lid, van de Tw, (kort gezegd): *voorafgaand aan het verkrijgen van uitdrukkelijke toestemming voor het aftappen, afluisteren 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, afluisteren, 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.
[322] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149-150.
[323] Idem, p. 149.
[324] Idem.
[325] 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.

Artikel 34 van de Wbp gaat er vanuit dat er geen onderzoeksplicht van de betrokkene is.[326]

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. 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 paragrafen 2.4 tot en met 2.6 (p. 22 e.v. van dit rapport) vastgesteld dat T-Mobile persoonsgegevens die ook verkeersgegevens zijn verwerkt voor de doeleinden netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie).

Het CBP heeft in paragraaf 3.5 (p. 56 e.v. van dit rapport) vastgesteld dat T-Mobile de persoonsgegevens die verkeersgegevens zijn, verzamelt met behulp van data-analyse apparatuur in haar mobiele netwerk. De persoonsgegevens worden (aldus) verkregen op een andere wijze dan bij de betrokkene.[327] Hetzelfde geldt voor virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

---

[326] Idem, p. 150.

[327] Zie ook *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149-150: *Artikel 34 regelt de situatie dat de gegevens op een andere wijze worden verkregen, dus buiten de betrokkene om, hetzij bij derden, bijvoorbeeld gegevens omtrent iemands kredietwaardigheid bij een handelsinformatiebureau, hetzij door eigen observatie, bij voorbeeld naar aanleiding van het gebruik van een netwerk in beheer van de verantwoordelijke*", (onderstreping toegevoegd door het CBP).

Het CBP heeft in de paragrafen 3.3 en 3.4 (p. 44 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 T-Mobile 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 T-Mobile de betrokkenen onder andere de doeleinden van de verwerking moet mededelen en 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.

T-Mobile informeerde betrokkenen in het oude Privacy Statement en de Algemene Voorwaarden niet volledig en niet duidelijk over de doeleinden van de verwerking, de categorieën gegevens die werden verwerkt, en over de duur van de verwerking (bewaartermijnen) (zie p. 82 e.v. van dit rapport).

De zinsnede in het oude Privacy Statement 'T-Mobile monitoort daarvoor niet jouw individuele gebruik van het netwerk' moet als feitelijk onjuist worden aangemerkt, althans is onvolledig en onvoldoende duidelijk. Verder kan T-Mobile niet volstaan met de mededeling dat gegevens (in abstracto) worden verwerkt om de kwaliteit van de dienstverlening te waarborgen: dit is te weinig specifiek. De betrokkene zal adequaat moeten worden geïnformeerd omtrent (in de woorden van de zienswijze 2 van T-Mobile): maatregelen genomen om congestie te voorkomen, om netwerkcapaciteit goed te plannen, om in staat te zijn om te onderzoeken of er ergens in het netwerk problemen zijn, zoals storingen of piekverbruik, om virussen en malware te bestrijden en om videoverkeer door middel van compressietechnieken op een voor gebruikers vriendelijke wijze mogelijk te maken, als het concrete doel van de gegevensverwerking als toetsingskader voor zorgvuldig gebruik.[328]

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 gegevensvergaring[329] in de vorm van data-analysetechnieken) en het gebruik dat ervan wordt/werd gemaakt, is het nodig dat T-Mobile de betrokkenen nadere informatie verstrekt(e) over de categorieën van

[328] Idem.
[329] Vgl. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 78.

verwerkte gegevens[330] en de bewaartermijn om tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen.[331]

Mededeling van de informatie aan de betrokkenen via een privacyverklaring/algemene voorwaarden op de T-Mobile website is/was mogelijk en kost geen onevenredige inspanning.

Het CBP heeft in paragraaf 3.6 (p. 58 e.v. van dit rapport) vastgesteld dat de *vastlegging* van de persoonsgegevens niet bij of krachtens de wet is/was voorgeschreven.

Doordat T-Mobile haar abonnees niet volledig en niet duidelijk informeerde over de hierboven genoemde drie doeleinden van de gegevensverwerking bij de toepassing van data-analysetechnieken en ook niet over de categorieën (soorten) van verwerkte gegevens en de bewaartermijn, handelde T-Mobile in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

Getroffen maatregelen

T-Mobile heeft haar privacy verklaring gewijzigd (versies april en december 2012).

Uit het voorgaande (zie p. 35 e.v. van dit rapport) blijkt dat T-Mobile in haar nieuwe Privacy Statement (versie april 2012) abonnees voor het eerst informeerde dat zij de continuïteit en integriteit van haar mobiele en vaste netwerken bewaakt. T-Mobile geeft aan daarvoor te onderzoeken of er bijvoorbeeld ergens in het netwerk van T-Mobile problemen voorkomen, zoals storingen of piekverbruik. Tevens informeerde T-Mobile over de categorieën van verwerkte persoonsgegevens die ook verkeersgegevens zijn ('gebruikers- en verkeersgegevens'). T-Mobile informeerde betrokkenen via het nieuwe Privacy Statement (versie april 2012) alleen in abstracto over bewaartermijnen: *"T-Mobile bewaart je persoonsgegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de doeleinden waarvoor T-Mobile je gegevens heeft verzameld. Hoe lang je gegevens worden bewaard is dus afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per (categorie van) gegeven(s) verschillen. T-Mobile bewaart in ieder geval je persoonsgegevens gedurende de looptijd van je abonnement en conform de wettelijke verplichtingen zoals genoemd onder 3.7. van dit Privacy Statement."*[332] Dit is onvoldoende specifiek.

Uit het voorgaande (zie p. 36 e.v. van dit rapport) blijkt dat T-Mobile in haar nieuwste Privacy Statement (versie december 2012) aanvullend informeert over dat zij onder andere 'bijhoudt' welke apps, websites en toepassingen haar klanten gebruiken, zodat zij extra capaciteit in kan zetten als dat nodig is én om data te comprimeren (zoals streaming video), dat zij geavanceerde technieken gebruikt die virussen kunnen herkennen om het netwerk en de klanten te beschermen tegen virussen, malware en andere aanvallen, alsmede analyseert welk toestel de betrokkene gebruikt en hoe dit toestel in haar netwerk functioneert, zoals het aantal succesvol opgezette

[330] Vgl. ook artikel 11, eerste lid, onder c, van de Privacyrichtlijn.
[331] Vgl. Last onder dwangsom NS Groep N.V. CBP 9 juni 2011, z2011-00057. URL: http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_NS.pdf (URL laatst bezocht op 29 mei 2013).
[332] T-Mobile Privacy Statement (versie april 2012).

verbindingen. Tevens informeerde T-Mobile over de categorieën van verwerkte persoonsgegevens die ook verkeersgegevens zijn (internetgegevens, welk toestel de klant gebruikt en hoe dit toestel in haar netwerk functioneert, toestelnummer (IMEI) of mobiele nummer, locatiegegevens enz.).[333]

Op deze punten is T-Mobile niet langer in overtreding (informatieplicht).

In het nieuwste Privacy Statement (versie december 2012) wordt over bewaartermijnen van persoonsgegevens opgemerkt: *"T-Mobile bewaart je persoonsgegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de doeleinden waarvoor T-Mobile je gegevens heeft verzameld. Hoe lang je gegevens worden bewaard is dus afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per (categorie van) gegeven(s) verschillen. In geval van een duidelijke en vaste bewaartermijn van gegevens is de specifieke bewaartermijn genoemd in de relevante paragraaf in dit Privacy Statement. Anders geldt dat T-Mobile in ieder geval je persoonsgegevens bewaart gedurende de looptijd van je abonnement en conform de wettelijke verplichtingen uit de Wet bescherming persoonsgegevens en Telecommunicatiewet."*[334] En: *"(…) nadat de relevante informatie uit het netwerk is gehaald worden de gegevens direct geanonimiseerd. T-Mobile kijkt niet naar de inhoud van jouw berichten of de door jouw bezochte websites*."[335] De zinsnede in het nieuwste Privacy Statement dat 'nadat de relevante informatie uit het netwerk is gehaald worden de gegevens direct geanonimiseerd' moet bijvoorbeeld wat betreft de gegevensverwerking via de [VERTROUWELIJK: apparatuur] voor het oplossen en voorkomen van netwerkproblemen als feitelijk onjuist worden aangemerkt, althans is onvolledig en onvoldoende duidelijk (zie hierover verder paragraaf 3.7, p. 80 e.v. van dit rapport).

Doordat de duur van de verwerking (bewaartermijnen) onvolledig en onvoldoende duidelijk zijn vermeld in het nieuwste Privacy Statement (versie december 2012) van T-Mobile, duurt de overtreding van artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp op dit punt voort.

3.9 Meldingsplicht

Uitwerking van het wettelijk kader

Artikel 27, eerste 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).

[333] T-Mobile Privacy Statement (versie december 2012).
[334] Idem.
[335] Idem.

Beoordeling

Het CBP heeft in paragraaf 3.7 'Uitdrukkelijk omschreven en gerechtvaardigde doeleinden' (p. 80 e.v. van dit rapport) vastgesteld dat T-Mobile de doeleinden - samengevat weergegeven - netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie) waarvoor zij persoonsgegevens verwerkt onvolledig en onvoldoende duidelijk had omschreven bij de meldingen met nummers m1070731 en m107067 (versienummer 5.0) die T-Mobile op 22 februari 2010 heeft gedaan.

Het CBP heeft in paragraaf 2.1 (p. 15-18 van dit rapport) vastgesteld dat T-Mobile geen andere meldingen had gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analysetechnieken in haar mobiele netwerk. De verwerkingen van persoonsgegevens door T-Mobile voor de hierboven genoemde doeleinden voldeden 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 (zie paragraaf 3.7, p. 80 e.v. van dit rapport). T-Mobile heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.

Doordat T-Mobile deze verwerkingen van persoonsgegevens niet had gemeld bij het CBP, handelde T-Mobile in strijd met artikel 27 jo. 28 van de Wbp.

Getroffen maatregelen

Het CBP heeft in paragraaf 3.7 'Uitdrukkelijk omschreven en gerechtvaardigde doeleinden' (p. 80 e.v. van dit rapport) vastgesteld dat T-Mobile de doeleinden netwerkplanning en -integriteit (waaronder netwerkplanning en -beheer, het oplossen en voorkomen van netwerkproblemen en virus- en malwarebestrijding), troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie) volledig en voldoende duidelijk heeft omschreven bij de gewijzigde meldingen van eind 2011 (versie 6.0) en - wat betreft de melding met nummer m1070731 - per eind oktober 2012. Hierdoor handelt T-Mobile niet langer in strijd met artikel 27 jo. 28 van de Wbp.

4. Conclusies

T-Mobile past data-analysetechnieken toe op het data- en signaleringsverkeer in haar mobiele netwerk.

Circa 2,8 miljoen T-Mobile abonnees met een (prepaid of postpaid) data abonnement maken gebruik van dataverkeersdiensten van T-Mobile.

T-Mobile verwerkt 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, websites en protocollen voor netwerkplanning en -beheer
- (technische) gegevens over het functioneren van het netwerk/toestel, zoals het aantal succesvol opgezette verbindingen
- URL's om [VERTROUWELIJK] compressie op video's toe te kunnen passen, tijdens de internetsessie van een abonnee
- virus- en malwareherkenningsgegevens uit (gedownloade) bestanden en verzonden en ontvangen e-mails
- (technische) gegevens over het functioneren van het netwerk/toestel om verzoeken om inlichtingen af te handelen, zoals verbruikte datavolume of het aantal succesvol opgezette verbindingen

Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn.

De persoonsgegevens worden door T-Mobile 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 T-Mobile direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon, omdat T-Mobile een koppeling(smogelijkheid) heeft met de unieke klant- en/of toestel identifier(s) (bijvoorbeeld het 06-nummer), 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 06-nummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume, IP-adres van-naar met poortnummer/protocol, locatiegegevens, URL's etc.
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens zijn), namelijk virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

T-Mobile inspecteert en analyseert 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

T-Mobile ook op inhoud teneinde virussen en malware tegen te houden en te verwijderen.

T-Mobile verwerkt de persoonsgegevens voor de volgende onderzochte doeleinden:

- netwerkbeheer en -integriteit (waaronder netwerkplanning en -beheer, virus- en malwarebestrijding en het oplossen en voorkomen van netwerkproblemen)
- troubleshooting (het oplossen van technische incidenten en klantproblemen in individuele gevallen)
- optimalisatie van de dienstverlening aan klanten (videocompressie).

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Één daarvan is bijvoorbeeld dat er altijd een wettelijke rechtvaardigingsgrond (grondslag) voor de gegevensverwerking moet bestaan. Het CBP heeft bij T-Mobile gedurende het onderzoek een aantal overtredingen van de Wbp én de Tw geconstateerd, die inmiddels gedeeltelijk zijn beëindigd.

Overtredingen die nog niet zijn beëindigd

Netwerkbeheer en -integriteit

Het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer 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.

T-Mobile verwijdert voor netwerkplanning en -beheer wat betreft één specifieke gegevensverwerking via de [VERTROUWELIJK: apparatuur] met betrekking tot websitebezoek of app- en protocolgebruik het verzamelde 06-nummer zo snel mogelijk. Omdat T-Mobile eventuele e-mailadressen niet zo snel mogelijk verwijdert, terwijl dat wel mogelijk is en was, heeft zij, na het verzamelen daarvan, toch geen grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit.

Omdat T-Mobile voor netwerkplanning en -beheer wat betreft een andere gegevensverwerking met betrekking tot hoogverbruik van data het verzamelde 06-nummer niet zo snel mogelijk verwijdert, terwijl dat wel mogelijk is en was, heeft zij, na het verzamelen daarvan, geen grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit.

T-Mobile handelt hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Overtredingen die gedeeltelijk zijn beëindigd

Informeren abonnees

T-Mobile 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. T-Mobile informeerde abonnees niet volledig en niet duidelijk over de volgende doeleinden van de gegevensverwerking bij de toepassing van data-analysetechnieken: netwerkbeheer en –integriteit en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie). Daarnaast informeerde T-Mobile hen niet over de categorieën (soorten) van verwerkte gegevens en de duur van de verwerking (bewaartermijnen). T-Mobile handelde hierdoor in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

T-Mobile heeft de privacyverklaring van het bedrijf aangepast, voor het laatst per december 2012.

T-Mobile informeert abonnees in haar nieuwste Privacy Statement (versie december 2012) niet volledig en niet duidelijk over de bewaartermijnen. T-Mobile handelt hierdoor nog in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

T-Mobile informeert abonnees in haar nieuwste Privacy Statement (versie december 2012) wel over de hiervoor genoemde drie doeleinden waarvoor zij persoonsgegevens verwerkt, evenals over de categorieën van verwerkte gegevens. Op deze punten handelt T-Mobile ten aanzien van de onderzochte gegevensverwerkingen niet langer in overtreding (informatieplicht).

Uitdrukkelijk omschreven en gerechtvaardigde doeleinden
Doordat T-Mobile de doeleinden waarvoor zij persoonsgegevens verwerkt bij aanvang van het onderzoek onvolledig en onvoldoende duidelijk had omschreven bij de meldingen die zij had gedaan en T-Mobile abonnees ook niet in haar oude Privacy Statement (versie april 2011) over de doeleinden netwerkbeheer en -integriteit en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie) informeerde, werden de door T-Mobile verzamelde persoonsgegevens in die laatste twee gevallen niet voor uitdrukkelijk omschreven doeleinden verzameld.

Doordat de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit (specifiek: netwerkplanning en -beheer en het oplossen en voorkomen van netwerkproblemen) bij aanvang van het onderzoek 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 T-Mobile verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld.

T-Mobile handelde hierdoor in strijd met 7 van de Wbp.

Doordat T-Mobile in haar gewijzigde meldingen en nieuwste Privacy Statement (versie december 2012) wel informeert over de drie doeleinden waarvoor zij persoonsgegevens verwerkt, handelt T-Mobile op dit punt niet langer in strijd met artikel 7 van de Wbp (uitdrukkelijk omschreven doeleinden).

De overtreding die inhoudt het verzamelen van persoonsgegevens zonder gerechtvaardigd doeleinde vanwege het verwerken zonder grondslag duurt voort

voor de gegevensverwerking voor netwerkplanning en -beheer via de [VERTROUWELIJK: apparatuur].

Doordat T-Mobile de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens voor het oplossen en voorkomen van netwerkproblemen inmiddels zo snel als mogelijk verwijdert, heeft zij in dat verband wel een grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit. Hierdoor handelt T-Mobile op deze punten niet langer in strijd met artikel 7 van de Wbp (gerechtvaardigde doeleinden).

Overtredingen die zijn beëindigd

Netwerkbeheer en -integriteit
Omdat T-Mobile voor het oplossen en voorkomen van netwerkproblemen de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens bij aanvang van het onderzoek niet zo snel als mogelijk na het verzamelen verwijderde, terwijl dat wel mogelijk is en was, had zij gedurende deze verwerkingsduur geen grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer en -integriteit. T-Mobile handelde hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Naar aanleiding van het onderzoek heeft T-Mobile de bewaartermijnen van de persoonsgegevens voor netwerkmonitoring via de [VERTROUWELIJK: apparatuur] verkort.

Doordat T-Mobile voor het oplossen en voorkomen van netwerkproblemen de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens inmiddels zo snel als mogelijk verwijdert, heeft zij in dat verband wel een grondslag voor de gegevensverwerking voor het doeleinde netwerkbeheer. Op die punten is T-Mobile niet langer in overtreding (grondslag).

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 T-Mobile waren bij aanvang van het onderzoek niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking netwerkbeheer en -integriteit, troubleshooting en optimalisatie van de dienstverlening aan klanten (waaronder videocompressie). T-Mobile handelde hierdoor in strijd met artikel 27 jo. 28 van de Wbp.

T-Mobile heeft de meldingen bij het CBP gewijzigd per eind 2011 en eind oktober 2012. Doordat T-Mobile de doeleinden van de gegevensverwerking alsnog heeft omschreven in de doelomschrijving in de gewijzigde meldingen die T-Mobile heeft gedaan, handelt T-Mobile ten aanzien van de onderzochte gegevensverwerkingen niet langer in strijd met de meldingsplicht.

Geen overtredingen geconstateerd

Virus- en malwarebestrijding, troubleshooting en videocompressie
T-Mobile heeft wel een wettelijke grondslag voor de verwerking ten behoeve van virus- en malwarebestrijding, troubleshooting en videcompressie. Op deze punten is T-Mobile dan ook niet in overtreding (geweest).

BIJLAGE I Overzicht mobiel netwerk

AFBEELDING 6 data-analyse apparatuur in mobiel netwerk T-Mobile[336]

[VERTROUWELIJK]

[336] Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, bijlage 1.

Netwerkplanning en -beheer ([VERTROUWELIJK: apparatuur])

[VERTROUWELIJK]
MSISDN (identificerend gegeven van de aansluiting: het 06-nummer) Let op: het 06-nummer wordt niet opgeslagen en bewaard.
hostname (URL op hoofddomein) van de website/app
URL van de website
IP-adres van-naar met poortnummer/protocol
e-mailadres van de T-Mobile abonnee die met een e-mail account van een aparte provider mailt of een derde die een T-Mobile klant mailt
start- en eindtijd sessie/tijdsvenster
verbruikte datavolume (aantallen bytes)
frequentie (het aantal keren dat verbinding wordt gemaakt)
[VERTROUWELIJK]
MSISDN (identificerend gegeven van de aansluiting: het 06-nummer)
verbruikte datavolume (aantallen bytes)

Ongewenst dataverkeer ([VERTROUWELIJK: apparatuur])

[VERTROUWELIJK identifier]
[VERTROUWELIJK]
inhoud van door abonnees (gedownloade) bestanden en ontvangen e-mails aan de hand van vooraf gedefinieerde virus- en malware-herkenningspatronen, voor zover nodig om virussen/malware tegen te houden en te verwijderen (virus- en malware-herkenningsgegevens)

Oplossen en voorkomen van netwerkproblemen ([VERTROUWELIJK: apparatuur])

[VERTROUWELIJK: identifiers]
VERTROUWELIJK
performance informatie/status (waaronder [VERTROUWELIJK])

Troubleshooting ([VERTROUWELIJK: apparatuur])

[VERTROUWELIJK: identifiers]
performance informatie / status (waaronder [VERTROUWELIJK])

Troubleshooting ([VERTROUWELIJK: apparatuur])

[VERTROUWELIJK: identifier]
[VERTROUWELIJK]

Videocompressie

[VERTROUWELIJK]
URL van de website om de gebruikte service [VERTROUWELIJK] te herkennen

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 afwikkelen 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 (*Gateway GPRS Support Node*)	Netwerkapparatuur die de signaleringen en het dataverkeer doorgeeft aan externe netwerken, zoals het internet.
GPRS (*General Packet Radio Service)*	Standaard voor het afwikkelen van mobiel dataverkeer.
GSM (*Global System for Mobile Communications*)	Standaard voor het afwikkelen van mobiel spraakverkeer. Sinds midden jaren negentig kan via GSM ook dataverkeer worden afgewikkeld. Dat wordt ook wel 2G-verkeer genoemd, *Second Generation Wireless Digital Technology*.
Hash	Wiskundige berekening die grotere dataverzamelingen van verschillende omvang kan omzetten naar kleinere dataverzamelingen met een vaste lengte.
HLR (*Home Location Register*)	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 (*International Mobile Equipment Identity)*	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 (*International Mobile Subscriber*	Voor klanten van mobiele telefonie

Identity)	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.
MSISDN (*Mobile Subscriber Integrated Services Digital Network-Number)*	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).
MVNO (*Mobile Virtual Network Operator*)	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).
SGSN (*Serving GPRS Support Node*)	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.
UMTS (*Universal Mobile Telecommunications Service*)	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.
VLR (*Visitor Location Register*)	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 IV Zienswijze 1 T-Mobile, met de reactie daarop van het CBP
(zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd én aangevuld met 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

OSI-model
Zienswijze 1 T-Mobile: T-Mobile schrijft in haar zienswijze 1 dat het CBP de bevinding dat T-Mobile zowel verkeersgegevens als inhoud van de communicatie verwerkt, baseert op een onjuiste weergave en analyse van het OSI-model. In haar zienswijze 1 merkt T-Mobile op dat ook in OSI-lagen 5 tot en met 7 sprake is van headers, en dat het ook in die lagen mogelijk is om informatie uit de headers te halen zonder dat er noodzakelijkerwijs sprake is van kennisneming van de inhoud van het verkeer (payload).[337]

T-Mobile voegt daaraan toe dat het OSI-model niets meer en niets minder is dan een hulpmiddel om processen in een telecommunicatienetwerk te kunnen duiden en zeker niet altijd en niet per definitie geschikt is om een adequate technische beschrijving te geven van daadwerkelijk gebruikte netwerken.[338] Voor een mobiel internet-netwerk wordt/moet worden uitgegaan van het TCP-IP-model. T-Mobile benadrukt: *"In dit model is het onderscheid tussen verschillende lagen minder duidelijk. Het komt erop neer dat er bij internetverkeer in verschillende lagen sprake kan zijn van header (envelop) en payload (inhoud). Ook om deze reden is het dus onjuist, althans te zeer ongenuanceerd, om ervan uit te gaan dat er wel of geen gegevens mogen worden verzameld uit de éne of de andere ISO/OSI-laag."*[339]

T-Mobile licht nader toe: *"Dit heeft onder andere betekenis bij VoIP diensten als Skype en bij op http gebaseerde streaming-diensten. Om allerlei reden (beveiliging of het voorkomen van blokkering of filtering) hebben de ontwikkelaars van deze diensten de gegevens waarmee het verkeer kan worden herkend ondergebracht in andere lagen dan op grond van het ISO/OSI-model wordt verondersteld. Om dit verkeer op een verantwoorde wijze te kunnen overbrengen aan haar abonnees en eindgebruikers is T-Mobile genoodzaakt gebruik te maken van netwerkmanagement-toepassingen die de vereiste gegevens ophalen uit verschillende lagen, zonder dat daarbij 'in de envelop' of naar 'de payload' wordt gekeken. Ook als deze gegevens uit laag 5, 6 of 7 worden gehaald is daarmee niet gezegd dat er sprake is van gegevens 'uit' het verkeer. Ook dan kan er sprake zijn van gegevens 'over' het verkeer."*[340]

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

[337] Zienswijze 1 T-Mobile, randnummers 17 en 21.
[338] Idem, randnummer 18.
[339] Idem, randnummer 19.
[340] Idem, randnummers 20 en 21.

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/*content*laag. 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."*[341]

Het CBP stelt niet dat het enkele feit dat T-Mobile ook gegevens uit de applicatielaag inspecteert en analyseert, zonder meer meebrengt dat T-Mobile tevens inhoud van de communicatie verwerkt.

Ten aanzien van een VoIP-dienst zoals Skype geldt echter, zoals T-Mobile in haar zienswijze ook aangeeft, dat de ontwikkelaars technische maatregelen hebben getroffen om herkenning van het verkeer te bemoeilijken, zoals het gebruik van 'betekenisloze headers', het dynamisch toewijzen van poorten en het versleutelen van de inhoud van berichten. Herkenning/identificatie van Skype-verkeer geschiedt daarom in de praktijk veelal door middel van uitgebreidere *signature based identification*. Dat wil zeggen, aan de hand van vooraf gedefinieerde patronen gebaseerd op de unieke eigenschappen van het protocol ('fingerprints'), zoals de lengte en de frequentie van verzonden en ontvangen packets bij de start van een Skype-sessie (bijvoorbeeld de eerste tien) in combinatie met (de eerste packets van de) inhoud van het verkeer/payload.[342]

---

[341] 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.

[342] Zie bijvoorbeeld Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, Paolo Tofanelli, 'Revealing skype traffic: when randomness plays with you', ACM SIGCOMM Conference - SIGCOMM 2007, p. 37-48. URL: http://dl.acm.org/citation.cfm?id=1282386. *"Following a closed source and proprietary design, Skype protocols and algorithms are unknown. Moreover, strong encryption mechanisms are adopted by Skype, making it very difficult to even glimpse its presence from a traffic aggregate."* en Dario Rossi, Marco Mellia, Michela Meo, 'Following Skype Signaling Footsteps', Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008.URL: http://www.tlc-networks.polito.it/oldsite/mellia/papers/skype-qosip.pdf: *"From a protocol perspective, Skype uses a proprietary solution which is difficult to reverse engineer due to extensive use of both cryptography and obfuscation techniques. Though Skype may rely on either TCP or UDP at the transport layer, both signaling and communication data are preferentially carried over UDP. A single random port is selected during application installation, and it is never changed (unless forced by the user). When a UDP communication is impossible, Skype falls back to TCP, listening to the same random port, and port 80 and 443 which are normally left open by network administrators to allow Web browsing."* P. Svoboda, E. Hyytia, F. Ricciato, M. Rupp, M. Karner, 'Detection and Tracking of Skype in a live 3G Network exploiting Cross Layer Information', 1st Int'l Workshop on Traffic Monitoring and Analysis (TMA 2009) 11 May 2009, Aachen, Germany. Published in LNCS vol. 5537. URL: http://publik.tuwien.ac.at/files/PubDat_184256.pdf. Zie bijvoorbeeld ook de recente guidance van het Nieuw-Zeelandse Cyber Security Centre over Skype. NCSC, Guidance

Verder geldt ten aanzien van virus- en malwarebestrijding dat T-Mobile de facto niet alleen headergegevens, maar ook inhoud van e-mails en bestanden inspecteert en analyseert om virussen en malware te herkennen.

De zienswijze 1 van T-Mobile heeft op het punt van (het gebruik van) het OSI-model geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. Zo is ter vergelijking het TCP-IP model opgenomen. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

[VERTROUWELIJK: apparatuur]
Zienswijze 1 T-Mobile: T-Mobile brengt naar voren dat het CBP in zijn beoordeling moet uitgaan van de feitelijk bij T-Mobile bestaande situatie (zoals die door T-Mobile aan het CBP is uiteengezet), niet van de fabrieksinstellingen van de gebruikte netwerkmanagement-toepassing en van wat zou blijken uit de bijbehorende standaarddocumentatie.[343] T-Mobile licht in haar zienswijze 1 nader toe dat via de [VERTROUWELIJK: apparatuur] gegevens over het daarlangs gaande dataverkeer kunnen worden opgehaald aan de hand van [VERTROUWELIJK].[344]

T-Mobile geeft in haar zienswijze 1 aan dat deze gegevens *"in enkele gevallen worden (…) verwerkt op het niveau van individuele eindgebruikers [VERTROUWELIJK] (…)."*[345]

T-Mobile merkt op dat zij voor netwerkplanning en -beheer gebruik maakt van [VERTROUWELIJK].[346]

T-Mobile schrijft: *"[VERTROUWELIJK]"*[347]

T-Mobile geeft aan dat aan de hand van [VERTROUWELIJK] de volgende gegevens worden geabstraheerd: [VERTROUWELIJK].[348] De gegevens worden ten hoogste 14 dagen bewaard.[349]

T-Mobile voegt toe over de [VERTROUWELIJK]: *"[VERTROUWELIJK]"*[350]

Reactie CBP: Bevindingen in hoofdstukken 2 en 3 van dit rapport zijn gebaseerd op de feitelijke instellingen van de gebruikte data-analyse apparatuur, zoals afgeleid uit de antwoorden van T-Mobile op de inlichtingenverzoeken van het CBP en OPTA (die zijn gecontroleerd aan de hand van de bijbehorende (product)documentatie) en

---

Regarding Skype and Other P2P VoIP Solutions, Ver. 1.1 June 2012. URL: http://ncsc.govt.nz/sites/default/files/articles/NCSC-Skype%20Guidance%201.1.pdf: *"Some P2P applications, such as Skype, use proprietary protocols and make use of encrypted tunnels to bypass firewalls. As a result, their use is extremely difficult to regulate or monitor."*
[343] Idem, randnummer 22.
[344] Idem, randnummer 26-27 en Annex, p. 13.
[345] Zienswijze 1 T-Mobile, randnummer 26.
[346] [VERTROUWELIJK]. Zienswijze 1 T-Mobile, Annex, p. 14.
[347] Zienswijze 1 T-Mobile, Annex, p. 14.
[348] [VERTROUWELIJK]
[349] Zienswijze 1 T-Mobile, Annex, p. 14.
[350] Idem, Annex, p. 15-16.

getoond tijdens het onderzoek ter plaatse van 17 oktober 2011.

De zienswijze 1 van T-Mobile heeft op het punt van (de werkwijze van T-Mobile bij) de inzet van data-analysetechnieken geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

Zienswijze 1 T-Mobile: T-Mobile benadrukt in haar zienswijze 1 dat [VERTROUWELIJK].[351]

T-Mobile schrijft in haar zienswijze 1: *"[VERTROUWELIJK]."*[352]

T-Mobile schrijft in haar zienswijze 1 dat zij voor dit doeleinde (ook) gebruik maakt van de [VERTROUWELIJK]. T-Mobile merkt op dat [VERTROUWELIJK]. De gegevens worden bewaard zolang dit nodig is om de aard en oorsprong van de aanval te kwalificeren (ten hoogste veertien dagen).[353]

T-Mobile geeft in haar zienswijze 1 aan dat zij voor dit doeleinde gebruik maakt van de [VERTROUWELIJK]. T-Mobile geeft aan dat aan de hand van de [VERTROUWELIJK] de volgende gegevens worden geabstraheerd: het volume aan verbruikte data per klant ([VERTROUWELIJK: identifier]) per sessie.[354] T-Mobile licht in haar zienswijze toe dat [VERTROUWELIJK]. Zit de gebruiker boven een bepaalde *threshold* (wettelijk, of op basis van zijn abonnement) dan [VERTROUWELIJK] een signaal naar de [VERTROUWELIJK: apparatuur], die de vereiste actie onderneemt (zoals een Speed Step Down naar [VERTROUWELIJK] of het blokkeren van toegang tot het internet in geval van roaming).[355]

Daarnaast worden aan de hand van de [VERTROUWELIJK] de volgende gegevens geabstraheerd: [VERTROUWELIJK].

T-Mobile schrijft dat er *"[VERTROUWELIJK] Deze gegevens worden maximaal 45 dagen bewaard."*[356]

Reactie CBP: De zienswijze 1 van T-Mobile heeft op het punt van (de werkwijze van T-Mobile bij) de inzet van data-analysetechnieken geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

Zienswijze 1 T-Mobile: T-Mobile schrijft in haar zienswijze 1: *"[VERTROUWELIJK]."*

[351] Zienswijze 1 T-Mobile, randnummer 27 en Annex, p. 16.
[352] Zienswijze 1 T-Mobile, Annex, p. 15-16.
[353] Zienswijze 1 T-Mobile, Annex, p. 15.
[354] Idem.
[355] Zienswijze 1 T-Mobile, Annex, p. 16.
[356] Zienswijze 1 T-Mobile, Annex, p. 13. Of T-Mobile een grondslag heeft voor de inzet van data-analysetechnieken ten behoeve van (handhaving van) de Fair Use Policy wordt/is niet door het CBP beoordeeld.

T-Mobile verwijst daarbij naar artikel 3.7 van de algemene voorwaarden die gebruikers accepteren wanneer ze gebruik maken van de gratis WiFi Hotspots: *"Peer-to-peer verkeer en streaming zijn niet mogelijk via T-Mobile HotSpot. De download- en uploadsnelheid van file transfer (FTP) wordt beperkt tot 128Kbps."*[357]

Reactie CBP: De vraag of er sprake is van herleidbaarheid van gebruikers van T-Mobile HotSpot in de trein is niet door het CBP onderzocht. De inzet van data-analysetechnieken valt buiten de scope van dit onderzoek voor zover het T-Mobile HotSpot in de trein betreft.

De zienswijze 1 van T-Mobile heeft op het punt van (de werkwijze van T-Mobile bij) de inzet van data-analysetechnieken geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

[VERTROUWELIJK: apparatuur]
Zienswijze 1 T-Mobile: T-Mobile benadrukt in haar zienswijze 1 dat het gebruik van de [VERTROUWELIJK: apparatuur] slechts betrekking heeft op gegevens betreffende de geslaagde en niet-geslaagde pogingen van abonnees en eindgebruikers (randapparatuur) om gebruik te maken van het netwerk van T-Mobile.[358] Volgens T-Mobile betreft de [VERTROUWELIJK: apparatuur] niet het gebruik van 'netwerk packet inspection' technologie en technieken en al helemaal niet het gebruik van technieken waarmee gegevens 'over' en 'uit' het mobiele dataverkeer worden geanalyseerd.[359] T-Mobile licht toe: *"[VERTROUWELIJK]."*[360]

T-Mobile schrijft in haar zienswijze 1 dat de [VERTROUWELIJK: apparatuur] door T-Mobile wordt gebruikt om connectiviteit op het netwerk van T-Mobile mee te monitoren en te beheren. [VERTROUWELIJK] Volgens T-Mobile kan worden geconcludeerd dat de [VERTROUWELIJK: apparatuur] niet kan worden gebruikt voor data-analysetechnieken op mobiel dataverkeer, of daarvoor in ieder geval niet wordt gebruikt door T-Mobile.[361]

Reactie CBP: Het CBP heeft T-Mobile bij brief van 18 augustus 2011 (aankondiging onderzoek) geschreven: *"Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) een ambtshalve onderzoek ingesteld naar de wijze waarop bij het gebruik van packet inspection technologie en technieken door T-Mobile Netherlands B.V. (T-Mobile) toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp."* En: *"Onder packet inspection technologie en technieken wordt in elk geval, maar niet uitsluitend, verstaan Shallow en Deep Packet Inspection."* In dit rapport zijn data-analyse techieken gedefinieerd als *"het gebruik maken van technieken waarmee gegevens over en uit het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd."* Met behulp van de [VERTROUWELIJK: apparatuur] worden packets geïnspecteerd en geanalyseerd. Gegevens over het functioneren van/de activiteit op het netwerk zijn

[357] Zienswijze 1 T-Mobile, Annex, p. 17.
[358] Zienswijze 1 T-Mobile, randnummer 31.
[359] Idem, randnummer 32.
[360] Idem, randnummers 22 en 32 tot en met 34.
[361] Idem, Annex, p. 18.

zulke gegevens over het mobiele dataverkeer. Dat zich ook probes bevinden in het radionetwerk (en dat niet alleen naar dataverkeer op het core netwerk wordt gekeken) maakt niet dat geen sprake is van packet inspection of dat de inzet van data-analysetechnieken op dit punt buiten de scope van het onderzoek zou vallen. T-Mobile heeft dit tijdens het onderzoek ook niet anders begrepen blijkens haar reacties op de verzoeken om inlichtingen, waarin zij is ingegaan op de [VERTROUWELIJK: apparatuur].

Verder wijst het CBP erop dat bevindingen in hoofdstukken 2 en 3 van dit rapport, zoals vermeld, zijn gebaseerd op de feitelijke instellingen van de door T-Mobile gebruikte data-analyse apparatuur, zoals afgeleid uit de antwoorden van T-Mobile op de inlichtingenverzoeken van het CBP en OPTA (die zijn gecontroleerd aan de hand van de bijbehorende (product)documentatie) en getoond tijdens het onderzoek ter plaatse van 17 oktober 2011.

De zienswijze 1 van T-Mobile heeft op het punt van (de werkwijze van T-Mobile bij) de inzet van data-analysetechnieken geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

Verwerking van persoonsgegevens

Zienswijze 1 T-Mobile: T-Mobile brengt in haar zienswijze 1 naar voren dat is voorzien in technische en organisatorische beveiligingsmaatregelen om een zorgvuldige en rechtmatige gegevensverwerking te waarborgen. Deze maatregelen betreffen een intern en extern (vanuit het moederbedrijf, en via onder andere externe audits) gehandhaafd beleid met betrekking tot functiescheidingen, beveiligingseisen, toegang tot applicaties en de verzamelde gegevens etc. Volgens T-Mobile wordt ook daarmee ervoor gezorgd dat de voor het netwerkbeheer vereiste gegevens beschikbaar zijn, alsmede dat deze gegevens alleen voor dat doel kunnen worden gebruikt door degenen die de gegevens daarvoor nodig hebben.[362]

Reactie CBP: Ten aanzien van de door T-Mobile gehanteerde technische en organisatorische maatregelen, waaronder Global Security Policies en de Privacy Code of Conduct van moedermaatschappij Deutsche Telekom AG, toegangsautorisaties (slechts een selecte groep medewerkers heeft toegang tot gebruik van de data analyse apparatuur), toegangsbeveiliging door middel van [VERTROUWELIJK][363], geldt dat dit bovenal een technische en organisatorische waarborg betreft ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp.[364] De omstandigheid dat slechts bepaalde medewerkers toegang hebben tot de data-analyse apparatuur en de data die met behulp daarvan wordt verwerkt, leidt echter niet tot de conclusie dat er geen sprake is van persoonsgegevens

[362] Zienswijze 1 T-Mobile, randnummer 9.
[363] Reactie T-Mobile op verzoek om inlichtingen van OPTA van 24 mei 2011, p. 3.
[364] Naleving van het bepaalde in artikel 13 van de Wbp (beveiliging) valt buiten de scope van dit onderzoek.

(er vindt geen anonimisering[365] of gegevensvernietiging plaats).

De zienswijze 1 van T-Mobile heeft op het punt van (algemene) technische en organisatorische maatregelen geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen dat T-Mobile persoonsgegevens verwerkt.

Zienswijze 1 T-Mobile: T-Mobile brengt in haar zienswijze 1 naar voren dat veel abonnees van T-Mobile ondernemingen en/of rechtspersonen zijn, en in de gevallen waarin deze zelf binnen de eigen organisatie zorgdragen voor de uitgifte van MSISDN's, SIM's etc. kunnen de betreffende eindgebruikers volgens T-Mobile niet worden geïdentificeerd, zodat geen sprake is van persoonsgegevens.[366]

Reactie CBP: 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 persoonsgegeven te beschouwen, bijvoorbeeld omdat de naam van de werknemer binnen dat bedrijf wordt vastgelegd. Ook gegevens over eenmanszaken en bedrijven handelend onder een eigennaam worden als persoonsgegevens aangemerkt, wanneer die ook iets zegt over het gedrag van de eigenaar.[367]

Daar komt bij dat het CBP hiervoor in dit Conceptrapport definitieve bevindingen gemotiveerd heeft vastgesteld dat de gegevensverwerking door T-Mobile mede is gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

De zienswijze 1 van T-Mobile heeft (daarom) op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen dat T-Mobile persoonsgegevens verwerkt.

<u>Samenloop Wbp en Tw: grondslagtoetsing</u>

Zienswijze 1 T-Mobile: T-Mobile merkt in haar zienswijze 1 op dat de in het

---

[365] Anonimiseren wordt in de wetsgeschiedenis bij de Wbp gedefinieerd als *"een vorm van vernietigen van persoonsgegevens althans in de gevallen dat de verwijdering van de naam ook tot gevolg heeft dat de betrokkene niet meer kan worden herleid. Alleen in dit laatste geval pleegt te worden gesproken van «anonimiseren»." Kamerstukken II* 1999/2000, 25 892, nr. 92c, p. 13.

[366] Zienswijze 1 T-Mobile, p. 9.

[367] Vgl. 'Klant in het web. Privacywaarborgen voor internettoegang', A&V-studie nr. 17, Registratiekamer juni 2000, p. 34 en 58. URL: http://www.cbpweb.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.

voorlopige rapport genoemde gegevensverwerkingen internetverkeersgegevens betreffen waarop allereerst artikel 11.5 Tw van toepassing is.[368]

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), volledige URL's en app/ protocol/service en 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, URL's en app/ protocol/service en virus- en malwareherkenningsgegevens

Ten aanzien van hostnames, URL's en app/ protocol/service en virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer, geldt dat geen sprake is van verkeersgegevens, maar van communicatie (tevens persoonsgegevens).[369] Artikel 8 van de Wbp is van toepassing, zij het dat (richtlijnconforme uitleg[370] 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.

Zienswijze 1 T-Mobile: In haar zienswijze 1 stelt T-Mobile 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), ter naleving van wettelijke verplichtingen (artikel 8, aanhef en onder c, van de Wbp) en ter behartiging van een gerechtvaardigd belang van T-Mobile, waarbij er geen sprake van is dat de belangen van de desbetreffende abonnees of eindgebruikers onevenredig worden aangetast (artikel 8, aanhef en onder f, van de Wbp).[371]

---

[368] Zienswijze 1 T-Mobile, randnummer 42.
[369] 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.
[370] 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*).
[371] Zienswijze 1 T-Mobile, randnummer 50 en 55-59.

T-Mobile betoogt in haar zienswijze 1 dat deze conclusie berust op een onhoudbare uitleg van de wet en dat het CBP uitgaat van een te beperkte opvatting over wat T-Mobile gehouden is te doen om uitvoering te geven aan de overeenkomsten met abonnees.[372] T-Mobile brengt in haar zienswijze 1 naar voren dat de door T-Mobile gebruikte netwerkmanagement-toepassingen zijn geconfigureerd voor haar specifieke mobiele internetnetwerk en de diensten die daarover worden aangeboden. Om haar abonnees de overeengekomen, betrouwbare en hoogwaardige mobiele diensten te kunnen aanbieden is dit volgens T-Mobile, in overeenstemming met de in de wetgeving gestelde eisen, op een zodanige wijze gedaan dat door gebruik van deze toepassingen niet te weinig, maar ook niet teveel gegevens over het netwerkgebruik beschikbaar zijn.[373] T-Mobile verwijst daarbij naar de instellingen van de verschillende netwerkmanagement-toepassingen en de andere technische en organisatorische beveiligingsmaatregelen om een zorgvuldige en rechtmatige gegevensverwerking te waarborgen, zoals een intern en zorgvuldige en rechtmatige gegevensverwerking te waarborgen: een intern en extern (vanuit het moederbedrijf, en via onder andere externe audits) gehandhaafd beleid met betrekking tot functiescheidingen, beveiligingseisen, toegang tot applicaties en de verzamelde gegevens etc.[374] T-Mobile benadrukt dat het CBP niet voorbij kan gaan aan de wijze waarop het gebruik van deze toepassingen in haar organisatie is ingebed en beveiligd.[375]

Reactie CBP: De verwerking van de persoonsgegevens is toelaatbaar indien deze noodzakelijk is voor 'uitvoering van een overeenkomst'. De toets is, onder andere, of de verwerking van persoonsgegevens, gelet op de hiervoor genoemde (andere) technische en organisatorische beveiligingsmaatregelen, 'noodzakelijk' en 'proportioneel'/'in overeenstemming met het subsidiariteitsbeginsel' is.

De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat een alternatief voor de door T-Mobile ingezette data-analyse apparaten dat ervoor zorgt dat gegevens direct onomkeerbaar worden geanonimiseerd op dit moment proportioneel is.

Zienswijze 1 T-Mobile: T-Mobile betwist dat er bij de huidige stand van zaken inderdaad 'andere manieren' zijn om de integriteit en –veiligheid van haar mobiele netwerk en diensten op een verantwoorde wijze te waarborgen.[376] T-Mobile voegt daaraan toe: *"Allereerst komt het T-Mobile voor dat het, in het licht van zijn wettelijke taakomschrijving, niet aan het College is om zich op dit detailniveau en zich in deze mate in te laten met haar bedrijfsvoering en de daarbij door haar te gebruiken apparatuur, toepassingen en instellingen. De veronderstelling dat een toezichthouder op deze wijze kan voorschrijven van welke apparatuur en toepassingen gebruik mag worden gemaakt, en op welke wijze en met welke instellingen dat zou mogen, verhoudt zich niet met een geliberaliseerde, op vrije marktverhoudingen gebaseerde concurrerende telecommunicatiemarkt."*[377] T-Mobile benadrukt zich, als aanbieder met meer dan tien jaar ervaring met mobiele

[372] Zienswijze 1 T-Mobile, randnummer 51-52.
[373] Idem 7.
[374] Idem, randnummers 8-9.
[375] Idem, randnummer 10.
[376] Zienswijze 1 T-Mobile, randnummer 15.
[377] Idem, randnummer 38.

internetnetwerken, goed geïnformeerd te achten over de beschikbare apparatuur en toepassingen, en de instellingen daarvan. In het licht daarvan acht zij het onwaarschijnlijk dat er (technische) alternatieven zijn, zonder dat er onacceptabele concessies worden gedaan aan netwerkintegriteit en -veiligheid.[378]

Reactie CBP: Het is (inderdaad) niet aan het CBP om zich op detailniveau in te laten met de door T-Mobile te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch alternatief voor te schrijven). Het is aan T-Mobile 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 voorgaande 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 worden ontdaan van persoonsidentificerende kenmerken. 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 T-Mobile heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat een alternatief voor de door T-Mobile ingezette data-analysetools dat ervoor zorgt dat verkeersgegevens direct onomkeerbaar worden geanonimiseerd op dit moment proportioneel is (de zienswijze 2 van T-Mobile heeft ten aanzien van de verwerking via de [VERTROUWELIJK: apparatuur] wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen).

Wettelijke plicht

Zienswijze 1 T-Mobile: T-Mobile betoogt dat nodig is dat gebruik wordt 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 en de roamingverordening.[379]

Reactie CBP: Artikel 20 van de Universeledienstrichtlijn (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)

[378] Idem, randnummer 39.
[379] Zienswijze 1 T-Mobile, randnummers 46 e.v.

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 transparantieverplichtingen. Uit dit artikel vloeit naar zijn aard geen wettelijke verplichting voort om met toepassing van data-analysetechnieken deze gegevens te verwerken. Er bestaat geen evident verband tussen de verwerking van de (gevoelige) persoonsgegevens op persoonsniveau, zoals die thans door T-Mobile plaatsvindt, en de transparantieverplichtingen. De inzet van data-analysetechnieken valt, zoals vermeld, buiten de scope van dit onderzoek voor zover het betrekking heeft op data roaming verkeer.

Indien en voor zover T-Mobile zich ten aanzien van het subdoeleinde bezoek en gebruik van apps, websites, protocollen en services 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 wetsartikelen[380], 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-analysetechnieken deze gegevens te verwerken. Er bestaat geen evident verband tussen de verwerking van de (gevoelige) persoonsgegevens op persoonsniveau, zoals die thans door T-Mobile 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 subdoeleinde een verplichting aan te nemen om met toepassing van data-analysetechnieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en (de uitvoering van) de wettelijke verplichting.

[380] Het CBP heeft de toepassing van de hieronder genoemde wetsartikelen voorgelegd aan OPTA en Agentschap Telecom in het kader van het Samenwerkingsprotocol CBP-OPTA onderscheidenlijk de Samenwerkingsovereenkomst Agentschap Telecom – College bescherming persoonsgegevens van beide toezichthouders. OPTA (thans: de ACM) en Agentschap Telecom stemmen elk voor zover zij ter zake de bevoegde toezichthouder zijn in met de voorgelegde toepassing van deze wetsartikelen.

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 subdoeleinde een verplichting aan te nemen om met toepassing van data-analysetechnieken (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 treedt in werking op 1 januari 2013.

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 T-Mobile rust en waarvan de verwerking met toepassing van data-analysetechnieken 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) is nog niet in werking getreden. 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-analysetechnieken (gevoelige) persoonsgegevens op persoonsniveau te verwerken. De uitzonderingen bepalen alleen 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.

De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat er geen wettelijke plicht is om met toepassing van data-analysetechnieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken voor verkeersbeheer.

Zienswijze 1 T-Mobile: T-Mobile geeft in haar zienswijze 1 aan dat niet kan worden uitgesloten dat zij in de nabije toekomst ook van data-analysetechnieken gebruik zal moeten maken om het verkeer van en naar als onrechtmatig gekwalificeerde bestemmingen te blokkeren of weg te filteren.[381]

Reactie CBP: Artikel 7.4a, eerste lid, aanhef en onder d, van de Tw (nieuw) geeft een uitzondering op de netneutraliteitsverplichting ter uitvoering van een wettelijk voorschrift of rechterlijk bevel. Dit artikellid biedt evenwel geen grondslag in de zin van de Wbp. Een grondslag voor de verwerking van persoonsgegevens, tevens communicatie moet worden gevonden in artikel 8 van de Wbp. De uitzonderingsgrond 'ter uitvoering van een rechterlijk bevel' correspondeert met de grondslag noodzaak (artikel 8, aanhef en onder f, van de Wbp).

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 subdoeleinde ter zake een verplichting aan te nemen om met toepassing van data-analysetechnieken 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 T-Mobile heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat er geen wettelijke plicht is om met toepassing van data-analysetechnieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken voor verkeersbeheer.

Technische alternatieven
Zienswijze 1 T-Mobile: T-Mobile betwist, zoals vermeld, dat er bij de huidige stand van zaken inderdaad 'andere manieren' zijn om de integriteit en -veiligheid van haar mobiele netwerk en diensten op een verantwoorde wijze te waarborgen.[382]

Reactie CBP: Het is, zoals vermeld, niet aan het CBP om zich op detailniveau in te laten met de door T-Mobile te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch

[381] Zienswijze 1 T-Mobile, voetnoot 4.
[382] Idem, randnummer 15.

alternatief voor te schrijven). Het is aan T-Mobile om onrechtmatige toepassingen van de data-analyse techniek te voorkomen. Op T-Mobile 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, 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.[383] T-Mobile 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. T-Mobile heeft de door het CBP aangedragen technische alternatieven onvoldoende specifiek weersproken. Het enkele feit dat T-Mobile niet bekend is met andere technische oplossingen (die direct toepasbaar zijn) binnen haar mobiele netwerk maakt niet dat de verwerking van persoonsgegevens zoals die thans door T-Mobile plaatsvindt proportioneel en subsidiair is.

De zienswijze 1 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat een alternatief voor de door T-Mobile ingezette data-analysetools dat ervoor zorgt dat verkeersgegevens direct onomkeerbaar worden geanonimiseerd op dit moment proportioneel is (de zienswijze 2 van T-Mobile heeft ten aanzien van de verwerking via de [VERTROUWELIJK: apparatuur] wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen).

Doeleinden

Zienswijze 1 T-Mobile: T-Mobile merkt in haar zienswijze 1 op dat zij meent dat bijvoorbeeld uit haar privacy statement, haar fair use policy en de overeenkomsten met abonnees voldoende duidelijk blijkt dat zij persoonsgegevens verwerkt om haar diensten te verlenen en om de kwaliteit daarvan te waarborgen, alsmede om overmatig netwerkgebruik tegen te gaan.[384] T-Mobile voegt daaraan toe: *"Inmiddels heeft T-Mobile evenwel zowel haar meldingen als haar privacystatements aangepast op een wijze die, naar zij aanneemt, tegemoet komt aan wat het College blijkens het voorlopig rapport van bevindingen van haar verlangt."*[385]

Reactie CBP: In de wetsgeschiedenis bij artikel 7 van de Wbp is over het begrip 'uitdrukkelijk omschreven' opgemerkt: *"Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen. In de gevallen dat hij op grond van artikel 29 van de melding is vrijgesteld, geldt het doel dat bij algemene maatregel van bestuur is omschreven op grond van artikel 29 tweede lid, onder a."*[386] Hieruit volgt dat de wetgever

[383] *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."*
[384] Zienswijze 1 T-Mobile, randnummers 63 en 67.
[385] Idem, randnummer 64.
[386] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 79.

heeft bedoeld dat het criterium in dit geval is of T-Mobile de doeleinden waarvoor zij persoonsgegevens verwerkt, heeft omschreven bij de (gewijzigde) meldingen die T-Mobile heeft gedaan. Niet is in de wetsgeschiedenis als criterium genoemd of uit het privacy statement, de fair use policy en de overeenkomsten van T-Mobile met abonnees voldoende duidelijk blijkt dat zij persoonsgegevens verwerkt voor deze doeleinden.

De overtreding van artikel 7 van de Wbp is niettemin inmiddels ten dele beëindigd, nu de doeleinden netwerkbeheer en -integriteit en troubleshooting door T-Mobile alsnog zijn omschreven bij de gewijzigde meldingen van 23 december 2011. Dat geldt niet voor het doeleinde optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie). De overtreding van artikel 7 van de Wbp duurt in zoverre voort.

De zienswijze 1 van T-Mobile heeft op het punt van het begrip 'uitdrukkelijk omschreven' doeleinden geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt, gelet op de gewijzigde meldingen, eveneens geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen. De zienswijze 2 van T-Mobile heeft op dit punt geleid tot aanpassing en verduidelijking van het toepasselijke en toegepaste wettelijk kader in het Rapport definitieve bevindingen.

Informatieplicht

Zienswijze 1 T-Mobile: T-Mobile betwist dat zij haar abonnees niet voldoende zou hebben geïnformeerd over de gegevensverwerkingen die plaatsvinden ten behoeve van het netwerkbeheer en het waarborgen van de netwerkintegriteit en -veiligheid.[387] T-Mobile meent dat zij heeft voldaan aan deze informatieverplichting in haar privacy statement en in de overeenkomsten met abonnees.[388] T-Mobile voegt daaraan toe dat zij *"in het kader van het voortdurende streven naar een nog duidelijke communicatie met haar abonnees en eindgebruikers, inmiddels haar privacystatement heeft aangepast. T-Mobile gaat er vanuit dat daarmee tegemoet is gekomen aan wat het College, blijkens haar voorlopig rapport, wenst."*[389] En: *"Er kan dan ook, zelfs als het in het definitieve rapport wordt vastgehouden aan het oordeel dat T-Mobile de wet zou hebben overtreden, geen ruimte meer zijn reparatoire sancties of andere maatregelen."*[390]

T-Mobile brengt in haar zienswijze 1 naar voren dat zij, in het kader van het voortdurende streven naar een nog duidelijkere communicatie met haar abonnees en eindgebruikers, haar privacy statement heeft aangepast.[391]

Reactie CBP: Het CBP heeft in dit Conceptrapport defnitieve bevindingen gemotiveerd vastgesteld dat sprake is van een overtreding van artikel 34 van de Wbp. Het CBP merkt op dat ook de Privacy Code of Conduct van moedermaatschappij

[387] Zienswijze 1 T-Mobile, randnummer 65.
[388] Idem, randnummer 66.
[389] Idem, randnummer 67.
[390] Idem, randnummer 74
[391] Zienswijze 1 T-Mobile, randnummer 67.

Deutsche Telekom AG bepaalt: *"[VERTROUWELIJK]."*[392]

De overtreding van artikel 34 van de Wbp is niettemin inmiddels ten dele beëindigd, nu het doeleinde van de verwerking 'voor netwerkbeheer en -integriteit', waaronder verstaan 'service management en het bewaken van service levels' en de categorieën van verwerkte persoonsgegevens, tevens verkeersgegevens door T-Mobile alsnog zijn beschreven in haar nieuwe Privacy Statement (versie april 2012). Dat geldt niet voor de (sub)doeleinden 'het vastleggen/bijhouden van individueel data ge-/verbruik en netwerkgebruik ten behoeve van het voorkomen van congestie/netwerkplanning en virus- en malwarebestrijding', 'videocompressie' en de categorieën van verwerkte persoonsgegevens, tevens communicatie. De overtreding van artikel 34 van de Wbp duurt in zoverre voort.

De zienswijze 1 van T-Mobile heeft op dit punt geleid tot aanpassing en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt, gelet op het gewijzigde Privacy Statement, eveneens geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen. De zienswijze 2 van T-Mobile heeft op dit punt geleid tot aanpassing en verduidelijking van het toepasselijke en toegepaste wettelijk kader, mede vanwege de afstemming van de wetsuitleg van artikel 11.5, vierde lid, van de Tw met Agentschap Telecom, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport.

<u>Meldingsplicht</u>

Zienswijze 1 T-Mobile: T-Mobile betwist dat zij de verwerking van persoonsgegevens ten behoeve van het netwerkbeheer en het waarborgen van netwerkintegriteit en -veiligheid niet zou hebben gemeld.[393] T-Mobile schrijft in haar zienswijze 1: *"In haar meldingen staat aangegeven dat de desbetreffende gegevens worden verwerkt ten behoeve van [doeleinden.. uitvoering overeenkomst]. Zoals in het voorgaande uiteengezet moet daaronder mede worden begrepen de gegevensverwerkingen ten behoeve van het netwerkbeheer en het waarborgen van netwerkintegriteit en -veiligheid. Dit was derhalve wel gemeld."*[394] T-Mobile brengt daarnaast naar voren dat de regeling van de meldplicht volgens haar vereist dat de verantwoordelijke adreswijzigingen binnen een week en andere wijzigingen binnen een jaar doorgeeft en dat T-Mobile, voor zover de gegevensverwerkingen indertijd niet zouden zijn gemeld, dat inmiddels - en ruim op tijd - heeft hersteld.[395] T-Mobile merkt ten slotte op dat artikel 28, vierde lid, van de Wbp[396] volgens haar uitdrukkelijk ruimte laat voor gegevensverwerkingen die afwijken van hetgeen bij het CBP is gemeld en dat, voor zover de gegevensverwerkingen indertijd niet zouden zijn gemeld, daarmee nog geen sprake is van een overtreding van de meldplicht.[397]

---

[392] E-mail T-Mobile aan OPTA van 30 mei 2011, bijlage. E-mail T-Mobile aan OPTA van 30 mei 2011: *"[VERTROUWELIJK]."*
[393] Zienswijze 1 T-Mobile, randnummer 68.
[394] Idem, randnummer 69.
[395] Idem, randnummers 70 en 71.
[396] Artikel 28, vierde lid, van de Wbp luidt: *"Een verwerking die afwijkt van hetgeen overeenkomstig het eerste lid, onder b tot en met f, is gemeld, wordt vastgelegd en bewaard gedurende ten minste drie jaren."*
[397] Zienswijze 1 T-Mobile, randnummer 72.

T-Mobile schrijft in haar zienswijze dat zij, zonder aanvaarding van enige gehoudenheid daartoe, enkele aanpassingen heeft aangebracht in haar privacy statements en meldingen.[398]

Reactie CBP: Het CBP heeft in dit Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat sprake is van een overtreding van artikel 27 jo. 28 van de Wbp.

Het CBP merkt daarnaast op dat artikel 28, derde lid, van de Wbp luidt: *"Een wijziging in de naam of het adres van de verantwoordelijke wordt binnen een week gemeld. Wijzigingen in de opgave die betrekking hebben op de onderdelen b tot en met f van het eerste lid* [te weten: onder andere het doel of de doeleinden van de verwerking en de beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben, toevoeging door het CBP], *worden telkens binnen een jaar na de voorafgaande melding gemeld voor zover zij blijken van meer dan incidentele aard te zijn"*, (onderstreping toegevoegd door het CBP). T-Mobile heeft de gewijzigde meldingen met nummers m1070731 en m1070767 (versienummer 6.0) gedaan op 23 december 2011. T-Mobile heeft de voorgaande meldingen met nummers m1070731 en m1070767 (versienummers 5.0) gedaan op 22 februari 2010. Hieruit volgt dat T-Mobile de wijzigingen - die niet van incidentele aard zijn - niet uiterlijk binnen een jaar na de voorgaande melding heeft gemeld.

In de wetsgeschiedenis bij de Wbp wordt over artikel 28, vierde lid, van de Wbp opgemerkt: *"De beoordeling of een wijziging al dan niet structureel is kan pas achteraf worden vastgesteld. Zolang de wijzigingen niet zijn doorgevoerd, dient de verantwoordelijke ingevolge het vierde lid de gegevens omtrent verwerkingen die niet geheel overeenstemmen met de melding, zelf op te slaan. Achteraf is aldus steeds vast te stellen aan bijvoorbeeld welke (categorieën van) ontvangers gegevens zijn verstrekt, dan wel of gegevens zijn doorgegeven aan landen buiten de Unie. Deze procedure voor melding van wijzigingen waarborgt aldus de transparantie van de gegevensverwerking."*[399] Dit artikellid stelt het bewijs veilig, zolang de melding niet is gewijzigd en laat, anders dan T-Mobile betoogt, niet 'uitdrukkelijk ruimte voor gegevensverwerkingen die afwijken van hetgeen bij het CBP is gemeld'.

De overtreding van artikel 27 jo. 28 van de Wbp is niettemin inmiddels ten dele beëindigd, nu T-Mobile de doeleinden netwerkbeheer en -integriteit en troubleshooting alsnog heeft gemeld bij het CBP. Dat geldt niet voor het doeleinde optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie). De overtreding van artikel 27 jo. 28 van de Wbp duurt in zoverre voort.

De zienswijze 1 van T-Mobile heeft op het punt van de meldingsplicht geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van T-Mobile heeft op dit punt, gelet op de gewijzigde meldingen, eveneens geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

[398] Zienswijze 1 T-Mobile, randnummer 74.
[399] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 139.

Bijlage V Zienswijze 2 T-Mobile, met de reactie daarop van het CBP

Scope: onduidelijkheid omtrent de reikwijdte en het onderwerp van onderzoek

Zienswijze 2 T-Mobile: in aanvulling op haar zienswijze 1, stelt T-Mobile in haar zienswijze 2 dat de reikwijdte van het onderzoek verschillende keren en op een voor T-Mobile niet inzichtelijke wijze is veranderd en opgerekt of verbreed. T-Mobile noemt ter illustratie dat in mei 2011 het onderzoek nog betrekking had op Deep Packet Inspection, in oktober 2011 op 'packet inspection', in januari 2012 ging het over 'data-analysetechnieken' op drie systemen en inmiddels is het onderzoeksdoel geworden 'het gebruik van technieken waarmee gegevens over en uit het mobiele verkeer kunnen worden geïnspecteerd en geanalyseerd' en wordt ook getoetst aan de bepalingen uit de Tw. De verandering en oprekking of verbreding van de onderzoeksdoeleinden duiden volgens T-Mobile op een *fishing expedition* en staan als zodanig op gespannen voet met zorgvuldigheidsvereisten, het verbod van willekeur en het verdedigingsbeginsel.[400]

Reactie CBP: Een fishing expedition waarbij via dwang ongericht informatie wordt verzameld, is in het kader een punitieve procedure (*criminal charge*) in het licht van het EVRM niet toegestaan.[401]

Het verbod van willekeur wordt wel geïnterpreteerd als het vereiste dat bestuursorganen beleid voeren. Het gevoerde beleid moet de toets aan het verbod van willekeur doorstaan (artikel 3:4 jo. 3:1 van de Awb).[402]

Het verdedigingsbeginsel omvat het recht dat iedere procespartij de kans moet krijgen zich behoorlijk te verdedigen.[403]

Veelal wordt aangenomen dat sprake is van een criminal charge vanaf het tijdstip waarop de overtreder uit handelingen van het bestuursorgaan redelijkerwijs kan afleiden dat hem een boete zal worden opgelegd/dat naar objectieve maatstaven door een redelijk waarnemer kan worden vastgesteld dat sprake is van een 'verhoor' met het oog op de oplegging van een bestuurlijke boete (zie artikel 5:10a van de Awb).[404] Vanaf dat tijdstip is hij niet meer verplicht ten behoeve van de boeteoplegging enige verklaring over de overtreding af te leggen.[405] In dit onderzoek (toezichtsfase) gaat het niet om een situatie waarin het bestuursorgaan overweegt om de overtreding 'punitief' af te doen. Om die reden is van een criminal charge in dit geval geen sprake.

---

[400] Zienswijze 2 T-Mobile, p. 1. Zie ook idem, p. 15 en 17.
[401] Zie o.a. EHRM 3 mei 2001, *AB* 2002, 343 (J.B. vs Zwitserland) en EHRM 21 april 2009, *NJ* 2009, 557 (Marttinen).
[402] *Commentaar Algemeen Bestuursrecht*, artikel 3:4 Awb, aantekening 1.2. Vgl. HR 25 februari 1949, *NJ* 1949, 558.
[403] Zie AbRvS 12 juli 2006, *AB* 2008, 144 dat het beginsel van *equality of arms* (partijen moeten gelijke kansen hebben om hun standpunten voor de rechter naar voren te brengen) als beginsel van behoorlijke rechtspleging niet ziet op bestuurlijke besluitvorming.
[404] Zie o.a. HR 17 februari 1987, *NJ* 1987/951; EHRM 27 februari 1980, *NJ* 1980/561 (Deweer); *Kamerstukken II* 2005/06, 29 702, nr. 7, p. 41 en *T&C Algemene wet bestuursrecht*, commentaar op artikel 5:10a Awb.
[405] Zie o.a. EHRM 17 december 1996, *NJ* 1997/699 (Saunders) en CRvB 21 november 2012, *AB* 2013, 27.

Evenmin is door de toezichthouders van het CBP buitensporig gezocht naar bewijs, zonder dat doel en voorwerp van het onderzoek nauwkeurig waren omschreven.

Er was een redelijke aanleiding zijn om op onderzoek uit te gaan. OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van artikel 10, eerste en derde lid, van het Samenwerkingsprotocol CBP-OPTA jo. artikel 24, tweede lid, van de Wet OPTA. In haar voorlopige bevindingen heeft OPTA hierover opgemerkt: "*Het is voor het college* [van de OPTA, toevoeging door het CBP] *nog niet duidelijk of de inzet van de door de aanbieders gebruikte analysemiddelen en de daarbij verwerkte gegevens in alle gevallen gerechtvaardigd en proportioneel is in het licht van de zorgplicht van artikel 11.2 Tw. (…) Daarvoor is nader onderzoek nodig. Het is daarbij van belang dat artikel 11.2 Tw nauw samenhangt met het bepaalde in de Wet bescherming persoonsgegevens, waarop het CBP toeziet. Het CBP en het college hebben hierover overlegd. Op grond van het samenwerkingsprotocol is besloten dat het college zijn bevindingen en de onderzoeksgegevens naar de naleving van artikel 11.2 van de Tw ter beschikking stelt aan het CBP. Het CBP zal deze bevindingen en de onderzoeksgegevens betrekken bij zijn onderzoek naar de naleving van de Wbp en de verwerking van persoonsgegevens bij de inzet van DPI-technieken."*[406]

In zijn aankondiging van het onderzoek heeft het CBP als reikwijdte en onderwerp van het onderzoek genoemd dat *het "een ambtshalve onderzoek* [heeft, toevoeging door het CBP] *ingesteld naar de wijze waarop bij het gebruik van packet inspection technologie en technieken* [voetnoot CBP: Onder packet inspection technologie en technieken wordt in elk geval, maar niet uitsluitend, verstaan Shallow en Deep Packet Inspection] *door T-Mobile Netherlands B.V. (T-Mobile) toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp."*

In (de aanbiedingsbrieven bij) het Rapport van voorlopige bevindingen en het Conceptrapport definitieve bevindingen is dit omschreven als *"de wijze waarop bij het gebruik van packet inspection technologie en technieken (data-analysetechnieken) door T-Mobile Netherlands B.V. (hierna: T-Mobile) toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp. Onderzocht is de verwerking van persoonsgegevens bij de data-analyse van gegevens over en uit het mobiele internetverkeer door T-Mobile", "de verwerking van persoonsgegevens over en uit het mobiele dataverkeer bij het gebruik van data-analysetechnieken door T-Mobile Netherlands B.V. (hierna: T-Mobile)" en "de wijze waarop T-Mobile Netherlands B.V. (hierna: T-Mobile) in haar mobiele netwerk packet inspection technologie en technieken (hierna: data-analysetechnieken) toepast".*

Het CBP heeft geen andere bescheiden of zaken (nader) onderzocht dan die welke verband houden met de wettelijke voorschriften waarop het toezicht in dit onderzoek betrekking heeft.

De zienswijze 1 van T-Mobile heeft ertoe geleid dat ook wordt getoetst aan bepalingen uit de Tw: *"Aan de specifieke normen van de telecommunicatiewetgeving, meer in het bijzonder de Telecommunicatiewet ("Tw") en de Roamingverordening ("Rvo"), wordt vrijwel volledig voorbijgegaan. Ten onrechte, omdat deze wetgeving zich tot de Wbp verhoudt als*

[406] 'Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken', *Onderzoek OPTA* 30 juni 2011.

specialis ten opzichte van de generalis. (…).”[407] In de aanbiedingsbrief bij het Conceptrapport definitieve bevindingen is daarover opgemerkt: *“Uw reactie heeft geleid tot aanpassing van de bevindingen ten aanzien van zowel de toepassingen en instellingen van de gebruikte data-analyse apparatuur als het toepasselijk wettelijk kader (samenloop Wbp en Telecommunicatiewet).”*

(Ook) naar aanleiding van de zienswijze 1 van T-Mobile dat het gebruik van de [VERTROUWELIJK: apparatuur] slechts betrekking heeft op gegevens betreffende de geslaagde en niet-geslaagde pogingen van abonnees en eindgebruikers om gebruik te maken van het netwerk van T-Mobile en dus niet betreft *“het gebruik van ‘netwerk packet inspection’ technologie en technieken en al helemaal niet het gebruik van technieken waarmee gegevens ‘over’ en ‘uit’ het mobiele internetverkeer worden geanalyseerd”*[408], heeft het CBP het Conceptrapport definitieve bevindingen verduidelijkt. Te weten: dat het gaat om de wijze waarop T-Mobile in haar mobiele netwerk packet inspection technologie en technieken (in het rapport gedefinieerd als data-analysetechnieken) toepast. Onder data-analysetechnieken wordt verstaan: technieken waarmee gegevens over en uit het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd. Het CBP stelt overigens vast dat T-Mobile in haar reactie op inlichtingenverzoeken van OPTA en het CBP er (wél) vanuit ging dat de [VERTROUWELIJK: apparatuur] een applicatie is waarmee datapakketten worden geanalyseerd.[409]

De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

Overtredingen volgens het rapport

Zienswijze 2 T-Mobile: T-Mobile gaat er in haar zienswijze 2 (onder meer) vanuit dat er volgens het CBP wel sprake is van een toereikende wettelijke grondslag én een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd verzameldoel voor zover T-Mobile persoonsgegevens verwerkt ten behoeve van het gebruik van firewalls en virusscanners, troubleshooting en videocompressie.[410] T-Mobile vat in haar zienswijze 2 samen dat volgens het CBP evenwel sprake is van een overtreding voor zover het gaat om het door T-Mobile verzamelen, gebruiken, vastleggen en bewaren van verwerkte persoonsgegevens over het bezoek aan en gebruik van apps, websites, protocollen en services. T-Mobile gaat er vanuit dat het CBP het niet meer nodig acht dat de abonnees over de gehanteerde bewaartermijn(en) worden geïnformeerd. Ten slotte is volgens het CBP sprake van overtreding van de meldplicht omdat niet volledig en/of niet voldoende duidelijk aan het CBP zou zijn gemeld dat T-Mobile persoonsgegevens verwerkt voor netwerkbeheer en -integriteit, troubleshooting en

[407] Zienswijze 1 T-Mobile, p. 8.
[408] Idem, p. 6.
[409] Zie o.a. Reactie T-Mobile op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2 en bijlage 1 bij deze reactie; Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3; Reactie T-Mobile op verzoek om inlichtingen van 19 september 2011, p. 2 (op de vraag naar de bewaartermijn van gegevens in, dan wel afkomstig uit de packet inspection apparatuur).
En bijlage 1 bij deze reactie.
[410] Zienswijze 2 T-Mobile, p. 1.

optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie).[411]

Reactie CBP: Anders dan T-Mobile meent, heeft het CBP in het Conceptrapport definitieve bevindingen geconcludeerd dat er géén uitdrukkelijk omschreven verzameldoel is (geweest) voor (onder meer) het doeleinde optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie).[412] In aanvulling op de hierboven staande samenvatting van T-Mobile merkt het CBP - volledigheidshalve - op dat (zoals T-Mobile blijkens haar zienswijze 2 ook begrijpt[413]) in het Conceptrapport definitieve bevindingen tevens een overtreding is geconstateerd van de verwerkingsgrondslag wat betreft het identificeren van trends in connectiviteit op het netwerk/handset performance voor service management en het bewaken van service levels via de [VERTROUWELIJK: apparatuur] (ofwel: 'het monitoren van haar (radio)netwerk en services ten aanzien van de beschikbaarheid en kwaliteit van de dienstverlening ter voorkoming van o.m. congestie en netwerkinterrupties'[414]). Anders dan T-Mobile stelt, acht het CBP (bovendien) nog steeds dat over de gehanteerde bewaartermijn(en) moet worden geïnformeerd.[415] Ten slotte wijst het CBP er op dat het in het Conceptrapport definitieve bevindingen alléén ten aanzien van het doeleinde optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie) een voortdurende overtreding van de meldingsplicht heeft geconstateerd.[416]

De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport. De zienswijze 2 van T-Mobile heeft (onder andere) op het punt van de noodzaak van de gegevensverwerking voor netwerkbeheer en -integriteit via de [VERTROUWELIJK: apparatuur] en gelet op de verkorting van de bewaartermijnen van de persoonsgegevens, wel geleid tot aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 2 van T-Mobile heeft daardoor eveneens geleid tot daarmee samenhangende wijziging(en) in de conclusie, namelijk dat het CBP ten aanzien van deze gegevensverwerking niet langer een overtreding constateert van het vereiste van een verwerkingsgrondslag.

<u>Onzorgvuldigheid (feiten)onderzoek</u>

Zienswijze 2 T-Mobile: T-Mobile meent dat het feitenonderzoek door het CBP ontoereikend is en dat het rapport ook in verschillende andere opzichten niet voldoet aan daaraan te stellen zorgvuldigheids- en andere vereisten (het verbod van willekeur en het verdedigingsbeginsel). Voor zover het CBP de conclusies van het Conceptrapport definitieve bevindingen in stand wenst te laten, kan dit volgens T-Mobile alleen worden gedaan na een aanvullend feitenonderzoek waarvan verslag wordt gedaan in een nieuw of substantieel gewijzigd rapport van bevindingen. T-

[411] Idem, p. 2. Zie ook idem, p. 10 en 17.
[412] Zie Conceptrapport definitieve bevindingen van 21 augustus 2012, p. 98-99 en 111.
[413] Zie o.a. Zienswijze 2 T-Mobile, p. 12-13 en 15.
[414] Reactie T-Mobile op vordering van 21 februari 2013, p. 3.
[415] Zie Conceptrapport definitieve bevindingen van 21 augustus 2012, p. 3, 103-104en 111.
[416] Idem, p. 107-108 en 111.

Mobile gaat er vanuit dat zij in de gelegenheid wordt gesteld om daarover nog haar zienswijze te geven.[417]

Feitenonderzoek
In het Conceptrapport definitieve bevindingen wordt volgens T-Mobile uitgegaan van onjuiste veronderstellingen onder andere over technische oplossingen die op dit moment niet beschikbaar zijn.[418] T-Mobile wijst in dat verband (kort gezegd) op de volgende punten.

T-Mobile veronderstelt dat het CBP zijn standpunt dat de gegevensverwerkingen niet nodig zijn voor het waarborgen van de veiligheid en integriteit van het netwerk onderbouwt met initiatieven gericht op het oplossen van capaciteitsproblemen in mobiele netwerken, bijvoorbeeld (blog)berichten dat telecomaanbieders en software-ontwikkelaars met elkaar in overleg zouden gaan, dat de GSM Association richtsnoeren zou hebben bekendgemaakt.[419]

Ten eerste bevestigen deze initiatieven volgens T-Mobile dat er sprake is van substantiële capaciteitsproblemen op mobiele netwerken. Hieruit kan (hooguit) worden opgemaakt dat er als gevolg van de snel toenemende databehoeftes van smartphone- en tabletgebruikers op dit moment sprake is van een exponentieel toenemende druk op het signaleringsnetwerk. T-Mobile verwijst ook naar andere bronnen. T-Mobile voegt daar in haar zienswijze 2 aan toe dat zij om die reden data-analyse toepassingen in gebruik heeft genomen. Ten tweede is volgens T-Mobile onduidelijk wat de relevantie is van deze initiatieven én een opmerking in een BEREC-rapport, waarin een relativerende kanttekening wordt geplaatst bij de verwachtingen met betrekking tot de groei van het dataverkeer.[420]

T-Mobile merkt in haar zienswijze 2 op dat uit het rapport niet blijkt of het CBP is uitgegaan van de feitelijke instellingen van de gebruikte data-analyse apparatuur.[421]

Wat betreft de door het CBP aangehaalde technische alternatieven heeft T-Mobile het CBP in haar zienswijze 1 verzocht (onder meer) inzichtelijk te maken wie dit onderzoek heeft verricht, op welke wijze dit is gedaan, wat daarvan de resultaten zijn, in hoeverre deze controleerbaar zijn, wat de specifieke alternatieven zijn en in hoeverre deze op een acceptabele wijze de netwerkintegriteit en -veiligheid waarborgen. T-Mobile brengt in haar zienswijze 2 naar voren dat dit in het Conceptrapport definitieve bevindingen niet is gebeurd. T-Mobile concludeert (daarom) dat onder andere onvoldoende onderzocht of de aangehaalde alternatieven wel 'andere mogelijkheden' of 'andere manieren zijn om hetzelfde doel te bereiken', in hoeverre deze feitelijk beschikbaar zijn en of deze oplossingen zonder onoverkomelijke risico's in het mobiele netwerk van T-Mobile kunnen worden geïmplementeerd, evenals de kosten van dergelijke oplossingen, de implicaties

[417] Zienswijze 2 T-Mobile, p. 3.
[418] Idem.
[419] Idem, p. 3-4. Zie ook idem, p. 7-8.
[420] Idem, p. 4.
[421] Idem, p. 3.

daarvan in termen van de betrouwbaarheid van de dienstverlening, de operationele gevolgen ervan, de eindgebruikerservaring etc.[422]

T-Mobile stelt dat in het Conceptrapport definitieve bevindingen (verder) niet wordt ingegaan op de argumenten van T-Mobile in haar zienswijze 1 dat het waarborgen van betrouwbare mobiele telecommunicatiediensten vereist dat er inzicht is in het netwerkgebruik van individuele eindgebruikers. Om dat te illustreren heeft T-Mobile gewezen op [VERTROUWELIJK]. Onder 'netwerkbeheer en -integriteit' moet (aldus) ook worden begrepen 'het voorkomen van congestie en monitoren van het netwerk'.[423]

T-Mobile brengt in haar zienswijze 2 naar voren dat het CBP van haar verlangt dat zij bewijst onschuldig te zijn. Het CBP construeert onder verwijzing naar (enkel) de parlementaire geschiedenis een 'diabolische bewijslast' die op gespannen voet staat met de beginselen van bewijslastverdeling, het verdedigingsbeginsel en de onschuldpresumptie. Het is aan het CBP om de feiten aan te dragen voor de beschikbaarheid van minder ingrijpende middelen waarmee bijvoorbeeld de persoonlijke levenssfeer van eindgebruikers meer of beter zou zijn gewaarborgd of een hoger niveau van dataminimalisatie zou kunnen worden bereikt, en daarin is het CBP volgens T-Mobile niet geslaagd.[424]

In haar reactie op de vordering van het CBP merkt T-Mobile op dat zij uit de verwijzing naar de gehoudenheid tot het beantwoorden van de gestelde vragen afleidt dat er inmiddels géén sprake meer is van verdenking van overtredingen en/of beboetbare feiten. Als dat ander is, kan de door T-Mobile in het kader van het onderzoek tot dusver verstrekte informatie (met inbegrip van deze reactie op de vordering) ter zake daarvan niet als bewijsmiddel dienen.[425]

Aanvullingen T-Mobile over nut en noodzaak van data-analyse in mobiele netwerken
In aanvulling op haar zienswijze 1 wijst T-Mobile op de continuïteitsverplichtingen en de afspraken die inmiddels[426] zijn gemaakt tussen KPN, T-Mobile en Vodafone om het telefoon- en sms-verkeer van elkaar overnemen bij een storing. Zo'n toename van het verkeersvolume kan alleen worden opgevangen als het netwerkverkeer voortdurend wordt gemonitoord. Omdat netwerkproblemen kunnen worden veroorzaakt door enkele gebruikers, en in voorkomende gevallen alleen kunnen worden opgelost door deze individueel te benaderen, kan daarvoor niet worden volstaan met onomkeerbaar geanonimiseerde gegevens.[427]

[422] Idem, p. 5.
[423] Idem, p. 5. Zie ook idem, p. 15-16 en 21-22 en de Annex bij deze zienswijze over de netwerkproblemen bij de introductie van de iPhone.
[424] Idem, p. 5-6. Zie ook idem, p. 14-15.
[425] Reactie T-Mobile op vordering van 21 februari 2013, p. 1-2.
[426] Zie o.a. *Kamerstukken II* 2012/13, 24 095, nr. 342 en 'Telecomproviders nemen dekking over bij storingen', *Nieuwsbericht Rijksoverheid* 7 mei 2013.
[427] Zienswijze 2 T-Mobile, p. 4. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 7.

Onzorgvuldigheden
Onder verwijzing naar haar zienswijze 1 wijst T-Mobile erop dat in het Conceptrapport definitieve bevindingen enerzijds bij de beschrijving van de feiten wordt verwezen naar bronnen waarvan de betrouwbaarheid twijfelachtig is (ongedateerde wikipedia-entries, blogberichten waaruit een onjuiste conclusie wordt getrokken) en anderzijds juiste bronvermeldingen en vindplaatsen ontbreken (een aantal URL's werkt bijvoorbeeld niet).[428]

T-Mobile merkt op dat in het Rapport voorlopige voorzieningen werd verwezen naar documenten waarvan de inhoud voor T-Mobile onbekend is (een gespreksverslag van OPTA van 26 mei 2011). T-Mobile heeft deze opgevraagd bij het CBP, maar nog niet ontvangen. In het Conceptrapport definitieve bevindingen zijn de verwijzingen naar dit verslag verwijderd. Onder verwijzing naar het verdedigingsbeginsel en een eerlijk proces stelt T-Mobile (echter) dat het CBP ofwel dit gespreksverslag aan haar moet verstrekken, ofwel de overwegingen die daarop zijn gebaseerd dient te verwijderen.[429]

T-Mobile meent dat het Conceptrapport definitieve bevindingen suggestieve en tendentieuze opmerkingen en verdachtmakingen bevat, die moeten worden verwijderd. T-Mobile wijst in dat verband op het gebruik van de term "oneigenlijk gebruik" van de gegevens zonder daarbij (ook) in te gaan op de maatregelen die T-Mobile heeft getroffen om te voorkomen dat daarvan sprake kan zijn én de verwijzing naar het WhatsApp-incident bij KPN.[430]

Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering
Reactie CBP: T-Mobile doet in haar zienswijze 2 een beroep op zorgvuldigheids- en andere vereisten (het verbod van willekeur en het verdedigingsbeginsel) en de onschuldpresumptie (artikel 6 van het EVRM). Zo heeft het CBP volgens T-Mobile onvoldoende onderzocht, althans niet deugdelijk gemotiveerd dat er andere mogelijkheden of andere manieren zijn om hetzelfde doel te bereiken zijn én of deze oplossingen zonder onoverkomelijke risico's in het mobiele netwerk van T-Mobile kunnen worden geïmplementeerd, evenals de kosten van dergelijke oplossingen, de implicaties daarvan in termen van de betrouwbaarheid van de dienstverlening, de operationele gevolgen ervan, de eindgebruikerservaring etc.

Zoals hierboven gemotiveerd (zie p. 117 van dit rapport), is van een criminal charge in dit onderzoek geen sprake.

De onschuldpresumptie en het uitgangspunt dat een verdachte niet hoeft mee te werken aan zijn eigen veroordeling (het nemo tenetur-beginsel) geldt vanaf het moment dat sprake is van een criminal charge.[431] In de toezichtfase kan de betrokkene nog geen beroep doen op dit beginsel. Er geldt daarom geen "onschuldpresumptie". T-Mobile heeft uit handelingen van het CBP in redelijkheid ook niet de verwachting kunnen ontlenen dat haar ter zake van de geconstateerde overtreding van de

[428] Idem, p. 7.
[429] Idem. Vgl. ook idem, p. 2.
[430] Idem, p. 8-9. Vgl. ook idem, p. 14.
[431] Zie o.a. EHRM 25 februari 1993, *NJ* 1993/485 (Funke) en AbRvS 19 september 1996, *AB* 1997, 91.

meldingsplicht een boete zal worden opgelegd. Er is T-Mobile geen cautie gegeven, in de aanbiedingsbrieven bij het Rapport voorlopige bevindingen en het Conceptrapport definitieve bevindingen is enkel opgemerkt *"Het CBP heeft de bevoegdheid om bestuursrechtelijke maatregelen te treffen zoals het opleggen van een last onder dwangsom bij voortduring van een geconstateerde onrechtmatigheid"* en het CBP heeft sinds 2007 geen boetes opgelegd ter zake van overtreding van de meldingsplicht[432] (wel is het CBP tegen overtredingen van de meldingsplicht in de laatste jaren opgetreden met een herstelsanctie[433]).

Ten aanzien van de 'reguliere' onderzoeksplicht in artikel 3:2 van de Awb geldt dat hoofdregel dat bij het nemen van een belastende beschikking de bewijs(voerings)last in beginsel op het bestuursorgaan rust. Niettemin kan zich de situatie voordoen dat bijvoorbeeld uit de parlementaire geschiedenis van een wetsartikel blijkt welke partij de bewijslast zou moeten dragen.[434] De plicht om de noodzaak van de verwerking aan te tonen berust onder het Wbp-regime bij de verantwoordelijke.[435] Ook de volgende factoren (vuistregels) kunnen de verdeling van de bewijslast beïnvloeden: de partij die belang heeft bij een bepaald feit, draagt de bewijslast, de partij in wier bewijsdomein het feit ligt, draagt de bewijslast en de partij die zich op een uitzondering of een verandering beroept, draagt de bewijslast.[436] In dat verband is relevant dat artikel 11.5 van de Tw een verwijderings-/anonimiseringsplicht bevat en T-Mobile zich op (een) uitzondering(en) daarop beroept.

Om aan de bewijs(voerings)last te voldoen, zal het bestuursorgaan onderzoek instellen naar de feiten. Het bestuursorgaan dient bij de voorbereiding van onder andere een besluit de nodige kennis te vergaren omtrent de relevante feiten en de af te wegen belangen (artikel 3:2 jo. 3:1 van de Awb). Bij ingrijpender besluiten worden in het algemeen zwaardere eisen aan het onderzoek gesteld. Neemt het bestuursorgaan een feitelijke stelling in, dan moet het deze stelling (vervolgens) met concrete feiten onderbouwen (geen schatting, subjectieve overtuiging of prognose, wel een

---

[432] URL: http://www.cbpweb.nl/downloads_jaarverslagen/jv_2012.pdf; http://www.cbpweb.nl/ downloads_jaarverslagen/jv_2011.pdf; http://www.cbpweb.nl/downloads_jaarverslagen/ jv_2010.pdf; http://www.cbpweb.nl/downloads_jaarverslagen/jv_2009.pdf; http://www.cbpweb.nl/downloads_jaarverslagen/jv_2008.pdf en http://www.cbpweb.nl/downloads_jaarverslagen/jv_2007.pdf. Zie ook http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf en http://www.cbpweb.nl/Pages/einde_vervolgprocedure_advance.aspx (URL's laatst bezocht op 29 mei 2013).

[433] URL: http://www.cbpweb.nl/Pages/pb_20110811_google.aspx en http://www.cbpweb.nl/downloads_pb/pb_20110419_brief_google_lod.pdf (URL's laatst bezocht op 29 mei 2013).

[434] Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005 , p. 111.

[435] *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."*

[436] Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005 , p. 137-141.

voldoende concreet en sterk vermoeden).[437] Heeft het bestuursorgaan de rechtsfeiten aannemelijk gemaakt - wordt vermoed dat de rechtsfeiten zich hebben voorgedaan, dan is het aan de belanghebbende om de onjuistheid van de vergaarde gegevens aannemelijk te maken.[438] Er mogen niet dermate zware eisen aan het vermoeden worden gesteld, dat de uitvoering van de bestuursbevoegdheid teveel wordt gefrustreerd.[439]

Het bestuursorgaan dat voornemens is een besluit te nemen, dient de belangen af te wegen die bij het besluit zijn betrokken. De voor een of meer belanghebbende nadelige gevolgen van het besluit mogen niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen (artikel 3:4 jo. 3:1 van de Awb).

Heeft een besluit negatieve consequenties dan zal het bestuursorgaan die nadelige consequenties moeten inventariseren. Op het bestuursorgaan rust ter zake een onderzoeksplicht. Voldoende is als het bestuursorgaan de betrokken belangen inventariseert en bij de belanghebbende navraagt in welke mate zijn belang door het voorgenomen besluit wordt geschaad. Het is aan de belanghebbende om aan de hand van bijzondere feiten en omstandigheden de schending van het evenredigheidsbeginsel aannemelijk te maken. De belanghebbende draagt de bewijslast voor de stelling dat zijn belang door het besluit onevenredig zwaar wordt getroffen.[440] Wel blijft het bestuursorgaan verantwoordelijk voor een deugdelijke belangenafweging.

Ten aanzien van de motiveringsplicht geldt dat de motivering het besluit moet kunnen dragen (artikel 3:46 jo. 3:1 van de Awb): een juiste vaststelling van de feiten die mag leiden tot het genomen besluit.[441]

Het CBP heeft zorgvuldig feitenonderzoek verricht.[442] Het CBP heeft T-Mobile bezocht en op verschillende moment gedurende het onderzoek inlichtingen en inzage in

---

[437] Idem, p. 91 en 104. Zie ook CBb 7 juli 2004, *LJN* AQ1048: *"Verweerder mag zijn oordeel dienaangaande mede baseren op vermoedens, mits deze vermoedens voldoende concreet en sterk zijn."*

[438] Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 103-104.

[439] Idem, p. 105. Zie ook CBb 29 april 2004, *AB* 2004, 317.

[440] Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 120. Zie o.a. AbRvS 15 oktober 1998, *JB* 1998, 278 en ABRS 18 september 2002, *AB* 2003, 132: *"(…) Dit neemt niet weg dat zich feiten en/of omstandigheden kunnen voordoen waardoor een individueel belang ten gevolge van een dergelijke maatregel zodanig zwaar wordt getroffen dat het bestuursorgaan, na afweging van de betrokken belangen, niet in redelijkheid tot het treffen van de verkeersmaatregel heeft kunnen besluiten, dan wel het nadeel daarvan redelijkerwijs niet ten laste van betrokkene dient te blijven. Dat sprake is van dergelijke feiten en omstandigheden dient in beginsel door betrokkene aannemelijk te worden gemaakt."*

[441] *T&C Algemene wet bestuursrecht*, commentaar op artikel 3:46 Awb.

[442] Zie over de zorgvuldigheid van het onderzoek AbRvS 15 augustus 2012, *LJN* BX4694: *"Anders dan De Koers ter zitting heeft betoogd, is er geen grond voor het oordeel dat de inspectie geen zorgvuldig feitenonderzoek heeft verricht. De inspectie heeft ter uitvoering van de tussenuitspraak De Koers op 30 september 2011 bezocht en gesprekken gevoerd met de directie, leerlingen, leraren, begeleiders en het bevoegd gezag. De inspectie heeft onderzocht welke leerbronnen de school inzet, heeft leerlingenwerk en leerlingendossiers bekeken en de door De Koers*

zakelijke gegevens en bescheiden gevraagd en vergaard van T-Mobile omtrent de wijze waarop de gegevensverwerking plaatsvindt, te weten: de categorieën van (soorten) gegevens, de verwerkingshandelingen, de duur van de verwerking, en daarmee samenhangend de configuratie-instellingen van de ingezette data-analyse apparatuur, alsmede voor welke doeleinden (zie het kopje 'Verloop onderzoek' voor een beschrijving van de ingezette toezichtshandelingen, waaronder het bekijken van (gebruikers)interfaces van de apparatuur die T-Mobile inzet voor data-analyse, p. 9 e.v. van dit rapport).

Het rapport bevat (daarnaast) een weerslag van verzamelde kennis op basis van de aanwezigheid van de vereiste expertise bij het bestuursorgaan zelf over mogelijkheden tot het niet langer beschikbaar houden (verwijderen) van gegevens met persoonsidentificerende kenmerken dan noodzakelijk is en het anonimiseren van persoonsgegevens. Gelet op deze kennis, in samenhang gezien met een analyse van de door T-Mobile beschikbaar gestelde inlichtingen en zakelijke gegevens en bescheiden omtrent de wijze waarop de gegevensverwerking plaatsvindt en voor welke doeleinden, heeft het CBP (daarna) gesteld dat er ten aanzien van bepaalde data-analysetechnieken (in het kader van het doeleinde netwerkbeheer en -integriteit) alternatieve maatregelen kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is (als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren). Vervolgens heeft het CBP op conceptueel niveau en in het Rapport voorlopige bevindingen ook met een concreet voorbeeld[443], onderbouwd hoe de informatiesystemen zouden kunnen worden vormgegeven, zonder (te) vergaand in te willen grijpen in de bedrijfsprocessen en bedrijfsvoering van T-Mobile. Gedacht kan worden aan bijvoorbeeld voor netwerkplanning en -beheer (waaronder mede begrepen het voorkomen van congestie en het monitoren van het netwerk) het toevoegen van een zogeheten privacy filter om gegevens met persoonsidentificerende kenmerken onmiddellijk na het verzamelen te verwijderen of onomkeerbaar te anonimiseren, zoals T-Mobile ook (grotendeels) toepast om met betrekking tot websitebezoek en app- en protocolgebruik het 06-nummer direct na het verzamelen te verwijderen. Van belang is daarbij waar het gaat om de haalbaarheid van zulke alternatieven dat het uitgangspunt van de Europese wetgever is geweest ten aanzien van het ontwikkelen van informatiesystemen voor de telecommunicatiemarkt dat deze *"systemen voor elektronische-communicatienetwerken en -diensten (…) op dusdanige wijze* [moeten, toevoeging door het CBP] *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 (...)"*, (overweging 30 van de e-Privacyrichtlijn).

Het CBP heeft T-Mobile tweemaal in de gelegenheid gesteld om op het bewijsmateriaal te reageren/tegenbewijs te leveren. T-Mobile heeft om de onjuistheid van de vergaarde gegevens aannemelijk te maken het volgende ingebracht. In haar

---

beschikbaar gestelde documenten geanalyseerd. Gezien deze onderzoeksactiviteiten is er geen reden voor het oordeel dat dit onderzoek onzorgvuldig is."

[443] Dit concrete voorbeeld is niet gehandhaafd in het Conceptrapport definitieve bevindingen.

zienswijzen 1 en 2, in onderling verband gelezen, heeft T-Mobile tegenbewijs geleverd in de vorm van (een) verklaring(en), onderbouwd met [VERTROUWELIJK].[444]

In haar zienswijzen 1 en 2 heeft T-Mobile (daarnaast) gesteld dat [VERTROUWELIJK]. T-Mobile heeft met haar zienswijzen op dit punt echter géén gerede twijfel opgewekt over de juistheid van de feitelijke stelling van het CBP dat er in algemene zin alternatieve maatregelen zijn die kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is. De geaggregeerde data bevat nog e-mailadressen in het geval een T-Mobile abonnee met een e-mailaccount van een (andere) provider mailt of een derde een T-Mobile klant mailt respectievelijk het verbruikte datavolume per top subscriber met wél nog het MSISDN (heavy user abonnee) (zie hierover verder p. 70 e.v. van dit rapport). T-Mobile heeft dit niet, althans onvoldoende onderbouwd weersproken.

Het CBP heeft de nadelige consequenties voor T-Mobile en (eventueel) haar klanten van het niet zo lang in niet-geanonimiseerde vorm mogen verwerken van de persoonsgegevens geïnventariseerd, bijvoorbeeld voor de netwerkintegriteit en stabiliteit, hoofdzakelijk beschreven in haar zienswijzen, en op een rij gezet in het rapport onder het kopjes 'Feitenonderzoek', 'Netwerkplanning en -beheer' en 'Connectiviteit op het netwerk/handset performance voor service management en bewaking van service levels' in deze **bijlage V** bij dit rapport. Naar aanleiding van de zienswijze 2 van T-Mobile heeft het CBP door middel van zijn vordering aan T-Mobile nagevraagd in welke mate zijn belang, bijvoorbeeld de netwerkintegriteit en stabiliteit, wordt geschaad als zij de persoonsgegevens niet zo lang in niet-geanonimiseerde vorm mag verwerken: *"of, in hoeverre en zo ja, op welke wijze andere factoren dan (de configuratie-instellingen op) de thans bij u in gebruik zijnde data-analyse apparatuur een rol spelen bij uw beantwoording van deze vraag naar de noodzaak om de gegevens over en/of uit het mobiele dataverkeer - ook na het verzamelen daarvan - in niet-geanonimiseerde vorm te verwerken, bijvoorbeeld congestierisico's of andere kwetsbaarheden die specifiek zijn voor uw netwerk(-infrastructuur)".* In haar reactie op de vordering van het CBP heeft T-Mobile daarover (louter) opgemerkt dat er voor netwerkplanning en -beheer geen gegevens worden gebruikt die direct of indirect herleidbaar zijn de individuele persoon. De vragen over een inschatting van de kosten (in euro's) en de tijd die het kost (in kalenderdagen) om (een) data-analyse oplossing(e) te (laten) ontwikkelen, implementeren en beheren die T-Mobile in staat zou stellen om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen te anonimiseren of zodanig te aggregeren dat deze niet met individuele klanten in verband kunnen worden gebracht dan wel om de verwerking van niet-geanonimiseerde gegevens te beperken tot die klanten die daarvoor hun (ondubbelzinnige) toestemming hebben gegeven, zijn daarom volgens haar niet relevant.[445] Wel heeft T-Mobile in haar zienswijze 2 genoemd dat alleen al de kosten van de *vervanging* van de in gebruik zijnde [VERTROUWELIJK: apparatuur]-apparatuur door andere (T-Mobile niet bekende of beschikbare) apparatuur moet worden [VERTROUWELIJK]. Wat betreft de doorlopende kosten kan volgens T-Mobile geen betrouwbare kosteninschatting worden gemaakt.[446]

[444] Zie Zienswijze 2 T-Mobile, p. 4 en de Annex bij deze zienswijze en Zienswijze T-Mobile van 12 februari 2012, p. 7. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 7.
[445] Reactie T-Mobile op vordering van 21 februari 2013, p. 4 e.v.
[446] Zienswijze 2 T-Mobile, p. 14.

De zienswijze 2 van T-Mobile heeft op het punt van de plicht tot zorgvuldige kennisvergaring en een zorgvuldige belangenafweging geleid tot aanvulling en verduidelijking van de relevante feiten en de geïnventariseerde en meegewogen belangen in dit rapport. De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Hoor en wederhoor
Voor zover T-Mobile zich in haar zienswijze 2 op het standpunt stelt dat het CBP niet een Rapport definitieve bevindingen kan vaststellen, maar haar (eerst) opnieuw gelegenheid dient te bieden tot het geven van zienswijzen, wijst het CBP op het volgende. (Louter) in uitzonderlijke gevallen zal een bestuursorgaan op grond van de algemene beginselen van behoorlijk bestuur verplicht zijn om indieners van zienswijzen in de gelegenheid te stellen een nieuwe zienswijze naar voren te brengen in verband met voorgenomen wijzigingen naar aanleiding van ingebrachte zienswijzen.[447] Daarvan is in dit geval geen sprake. T-Mobile heeft al tweemaal kunnen reageren op het rapport. T-Mobile is door de wijzigingen naar aanleiding van haar zienswijze (ook) niet in haar belangen geschaad. De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

Feitelijke instellingen van de gebruikte data-analyse apparatuur
Waar T-Mobile in haar zienswijze 2 opmerkt dat uit het Conceptrapport definitieve bevindingen niet blijkt of het CBP is uitgegaan van de feitelijke instellingen van de gebruikte data-analyse apparatuur, wijst het CBP erop dat dit onder andere blijkt uit de bronvermeldingen. Het CBP heeft de feitelijke bevindingen met name vastgesteld aan de hand van de inlichtingen van T-Mobile (veelal verklaringen gedurende het onderzoek) omtrent de categorieën van (soorten) verwerkte gegevens, de verwerkingshandelingen, de duur van de verwerking, en daarmee samenhangend de configuratie-instellingen van de ingezette data-analyse apparatuur, alsmede voor welke doeleinden, en de screenshots gemaakt tijdens het onderzoek ter plaatse. Voor zover T-Mobile heeft verwezen naar (product)documentatie ([VERTROUWELIJK]), zijn de daarin genoemde configuratie-instellingen als uitgangspunt genomen.

De zienswijze 2 van T-Mobile heeft op dit punt geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Aanvullingen T-Mobile over nut en noodzaak van data-analyse in mobiele netwerken
De zienswijze 2 van T-Mobile heeft op het punt van de aanvullingen van T-Mobile over nut en noodzaak van data-analyse in mobiele netwerken geleid tot aanvulling van de feitelijke bevindingen in het rapport.

Bronvermeldingen en gespreksverslag OPTA

[447] CBb 3 november 2009, *AB* 2009, 402.

Op het punt dat T-Mobile bezwaar maakt tegen (de vorm van) de bronvermeldingen geldt dat er geen wettelijk voorschrift of algemeen rechtsbeginsel is dat meebrengt dat in een rapport als dit niet mag worden verwezen naar Wikipedia uitleg of blogberichten.

Voor zover T-Mobile meent dat het CBP in het Conceptrapport definitieve bevindingen een overtreding van de verwerkingsgrondslag zou hebben geconstateerd (louter) op basis van (blog)berichten dat telecomaanbieders en software-ontwikkelaars met elkaar in overleg zouden gaan en dat de GSM Association richtsnoeren zou hebben bekendgemaakt, geldt dat dit niet juist is. Uit het rapport kan zulks ook geenszins worden opgemaakt.

Zoals vermeld, dient het bestuursorgaan bij de voorbereiding van onder andere een besluit de nodige kennis te vergaren omtrent de relevante feiten en de af te wegen belangen (artikel 3:2 jo. 3:1 van de Awb). Dit betekent dat het bestuursorgaan niet alleen onderzoek heeft ingesteld naar de werkwijze van T-Mobile bij de inzet van data-analysetechnieken, de noodzaak daartoe (bijvoorbeeld op het punt van de netwerkbelasting en de verwachte toename daarvan) en mogelijke technische alternatieven, maar ook heeft bekeken en kennis heeft genomen van of en in hoeverre er (gedeeltelijk) andere mogelijkheden zijn om de oorzaak van het probleem aan te pakken.

Ten aanzien van het gespreksverslag van OPTA geldt dat dit niet ten grondslag is gelegd aan de bevindingen en conclusies in het (Concept)rapport definitieve bevindingen.[448] In het rapport wordt ook niet daarnaar verwezen. T-Mobile wordt reeds daarom niet in haar belangen geschaad. Op verzoek van het CBP is door de ACM besloten om bij eenmalige uitzondering toe te staan om (een deel van) het gespreksverslag van T-Mobile/OPTA door het CBP te laten verstrekken aan T-Mobile. Het CBP beschikt niet over andere 'documenten waarvan de inhoud voor T-Mobile onbekend is'.

De zienswijze 2 van T-Mobile heeft op het punt van de door het CBP aangehaalde relativering door BEREC van de toename in dataverkeer en andere initiatieven en activiteiten om de druk op het signaleringskanaal te verminderen, geleid tot nuancering van het belang daarvan in de feitelijke bevindingen in het rapport. De zienswijze 2 van T-Mobile heeft op het punt van de Wikipedia uitleg geleid tot aanvulling van de datum laatste bezoek aan de betreffende webpagina. De zienswijze T-Mobile heeft op dit punt voor het overige niet geleid tot aanpassingen van de feitelijke bevindingen en conclusies in het rapport.

Neutrale bewoordingen
Het CBP wijst er op dat het rapport steunt op voldoende concrete en objectieve gegevens. Het onderzoek van het CBP was gericht op waarheidsvinding, ofwel het verzamelen van zowel 'belastende' als 'ontlastende' informatie. Zo heeft het CBP kennis vergaard over zowel de werkwijze van T-Mobile bij de inzet van data-analysetechnieken, de noodzaak daartoe (bijvoorbeeld op het punt van de netwerkbelasting en de verwachte toename daarvan) en mogelijke alternatieven.

[448] Zie ook E-mail CBP van 10 februari 2012 aan T-Mobile.

Uit zorgvuldigheid en om misverstanden te voorkomen, is de verwijzing naar de algemene neergang van spraakverkeer en SMS en de noodzaak om nieuwe business modellen op te stellen (inclusief de verwijzing naar het WhatsApp-incident bij KPN) (evenwel) weggelaten uit dit Rapport definitieve bevindingen. De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Geen overtreding van de Wbp en/of Tw

Zienswijze 2 T-Mobile: T-Mobile meent dat bij geen van de in het rapport beoordeelde gegevensverwerkingen sprake is of was van overtredingen van de Wbp en/of Tw (zij verwijst daarbij ook naar haar zienswijze 1).[449] Op het gebied van de beoordeling van de gegevensverwerkingen door het CBP wijst T-Mobile op het volgende.

Consistentie terminologie
Volgens T-Mobile is het Conceptrapport definitieve bevindingen niet eenduidig over wat volgens het CBP als overtreding moet worden gekwalificeerd.[450] Onder verwijzing naar haar zienswijze 1 merkt T-Mobile op dat het CBP om onduidelijke redenen en ten onrechte is afgeweken van onder andere de door T-Mobile gebruikte doelomschrijving 'netwerkbeheer en -integriteit': bijvoorbeeld met de omschrijvingen 'netwerkplanning en -beheer', 'netwerkplanning en *forecasting*', 'om inzicht te hebben/krijgen in de ontwikkelingen van het verkeer, netwerkgebruik etc. in verband met de netwerkbelasting' en 'om trends in gebruikersverkeer te identificeren, voor netwerkplanning (forecasting) respectievelijk trends in connectiviteit op het netwerk/*handset performance* voor service management en het bewaken van *service levels'* (wat leidt tot een stroman drogreden).[451] Ook spreekt het rapport zichzelf volgens T-Mobile af en toe tegen.[452] Omdat de conclusie van het CBP dat er een overtreding is met betrekking tot de verwerkingsgrondslag niet (logisch) uit het Conceptrapport definitieve bevindingen volgt, is het naar de mening van T-Mobile niet goed mogelijk om te duiden welke verwerkingen door het CBP als overtreding worden aangemerkt, wat daarvan de omvang is en welke maatregelen nodig zouden zijn om deze te beëindigen. In haar zienswijze 2 houdt T-Mobile het er (vooralsnog) onder meer op dat zij *"begrijpt dat het College vindt dat er sprake is van een overtreding van het bepaalde in artikel 11.5 Tw jo. 8 Wbp met betrekking tot de verwerkingen die plaatsvinden ten behoeve van wat het College aanduidt als (a) netwerkplanning (forecasting) respectievelijk (b) trends in connectiviteit op het netwerk/handset performance voor service management en het bewaken van service levels. (…)."*[453]

T-Mobile stelt in haar zienswijze 2 dat het CBP de begrippen "verwerkingsdoeleinden" en "verwerkingsgrondslagen" door elkaar lijkt te halen.[454]

[449] Zienswijze 2 T-Mobile, p 2.
[450] Idem, p. 10.
[451] Idem, p. 5. Zie ook idem, p. 10 en 13-14. Zie ook Reactie T-Mobile op vordering van 21 februari 2013, p. 2-3 en 7.
[452] Zienswijze 2 T-Mobile, p. 10.
[453] Idem, p. 12. Zie ook idem, p. 13.
[454] Idem, p. 10.

T-Mobile vindt onduidelijk wat het CBP bedoelt met 'het gebruiken van persoonsgegevens op individueel niveau'. T-Mobile gaat ervanuit dat het CBP bedoelt te zeggen dat sprake is van de verwerking van persoonsgegevens en niet van geanonimiseerde en geaggregeerde gegevens.[455]

T-Mobile acht het verwarrend dat in het Conceptrapport definitieve bevindingen met de term "grondslag noodzaak" wordt gedoeld op de grondslag als genoemd in artikel 8, aanhef en onder f, van de Wbp (noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke).[456]

Opbouw, structuur en argumentatie van het rapport
T-Mobile meent dat waar het gaat om de gestelde overtreding met betrekking tot de verwerkingsgrondslag de structuur van het rapport onduidelijk is en de argumentatie moeilijk te volgen, vooral doordat feitelijke, opiniërende en normatieve beschrijvingen door elkaar lopen (en het ontbreken van eindredactie?).[457] Verder lijkt er sprake van een *one-size-fits-all* benadering die geen recht doet aan de concrete en specifieke omstandigheden van T-Mobile.[458] Dit alles staat volgens T-Mobile op gespannen voet met de vereisten die voortvloeien uit het zorgvuldigheids-, verdedigings-, en lex certa-beginsel (rechtszekerheidsbeginsel), alsmede het verbod van willekeur en de onschuldpresumptie.[459]

Overige opmerkingen
T-Mobile merkt in haar zienswijze 2 op dat de enkele stelling dat een passende beveiliging van de gegevens niet mogelijk zou zijn op gespannen voet staat met artikel 13 van de Wbp en artikel 11.3 van de Tw en áls er is voorzien in een passende beveiliging, de verzameling en verwerking niet om die reden als strijdig met artikel 7 of 8 van de Wbp kan worden gekwalificeerd.[460]

T-Mobile betwist dat de verwijzing naar het arrest van het Hof van Justitie van 16 december 2008 (Huber) relevant is. Zij meent dat dit en de daarop voortbouwende argumentatie een stroman drogreden is, in strijd met het zorgvuldigheids- en motiveringsbeginsel en het verbod op vooringenomenheid. T-Mobile verzamelt geen gegevens op basis van een wettelijke bevoegdheid tot statistische gegevensverwerking, maar omdat zij deze gegevens nodig heeft voor haar netwerkbeheer en -integriteit, waaronder mede begrepen het waarborgen van de veiligheid van het netwerk, het oplossen en voorkomen van netwerkproblemen, het voorkomen van congestie door forecasting etc. Deze gegevens worden vervolgens door haar geanonimiseerd en geaggregeerd. Op basis van de geaggregeerde gegevens worden vervolgens niet tot individuele gebruikers herleidbare statistieken samengesteld.[461]

[455] Idem.
[456] Idem, p. 11 en 13.
[457] Idem, p. 13.
[458] Idem, p. 10 en 13.
[459] Idem, p. 13.
[460] Idem, p. 9.
[461] Idem.

T-Mobile meent dat de verwijzing naar artikel 11.2a van de Tw niet ter zake doend is.[462]

Netwerkplanning en -beheer
Onder verwijzing naar haar zienswijze 1 benadrukt T-Mobile dat voor het 'subdoeleinde' netwerkplanning en -beheer (waaronder mede begrepen het voorkomen van congestie en het monitoren van het netwerk) een beperkt aantal gegevens is vereist. Deze verkrijgt T-Mobile via de [VERTROUWELIJK: apparatuur], en met behulp van [VERTROUWELIJK]. T-Mobile meent dat zij aldus heeft voldaan aan wat de wet van haar verlangt (onomkeerbaar geanonimiseerde en geaggregeerde gegevens en een voldoende niveau van dataminimalisatie). Dit ook omdat het implementeren van andere middelen, ook gelet op het huidige (hoge) niveau van bescherming en dataminimalisatie, in termen van privacybescherming niet meer dan een marginale meerwaarde heeft, terwijl de financiële en bedrijfseconomische en andere kosten aanmerkelijk zijn.[463] T-Mobile voegt in haar reactie op de vordering van het CBP daaraan toe: *"In het kader van dit subdoeleinde kijkt T-Mobile op basis van volume en type (signalering)verkeer naar trends en ontwikkelingen die (verwacht worden) zich voor (te) doen, en die aanleiding kunnen zijn om de netwerkcapaciteit aan te passen. Deze analyse wordt door T-Mobile niet gedaan op basis van de IP analyse technieken waarop het onderzoek van uw College is gericht. Voor (de langere termijn) netwerkplanning worden door T-Mobile geen gegevens gebruikt die direct of indirect herleidbaar zijn tot de individuele persoon."*[464]

T-Mobile schrijft in haar zienswijze 2 dat alleen al de kosten van de *vervanging* van de in gebruik zijnde [VERTROUWELIJK: apparatuur]-apparatuur door andere (T-Mobile niet bekende of beschikbare) apparatuur moet worden [VERTROUWELIJK]. Wat betreft de doorlopende kosten kan volgens T-Mobile geen betrouwbare kosteninschatting worden gemaakt. Met het realiseren van de extra netwerkcapaciteit die nodig is om netwerkproblemen te voorkomen die het gevolg zouden zijn van verminderd inzicht in de werking van het netwerk zullen ten minste [VERTROUWELIJK] zijn gemoeid. Zulke kosten worden uiteindelijke doorbelast aan de abonnees, aldus T-Mobile.[465] Als 'andere kosten' noemt T-Mobile vervroegde afschrijvingen van de thans in gebruik zijnde apparatuur, implementatiewerkzaamheden, sterk verminderde stabiliteit en betrouwbaarheid van het netwerk, sterk verminderde gebruikservaring, afhandeling van extra klachten als gevolg van een instabiel en minder betrouwbaar netwerk, verminderde bereikbaarheid van abonnees en eindgebruikers (én het alarmnummer 112).[466]

T-Mobile wijst er in haar zienswijze 2 (bovendien) op dat de planning en het beheer van het netwerk behalve forecasting ook andere activiteiten van beheer omvat. Het gaat dan om het monitoren van verschillende verkeersstromen en zogenaamde '*load*'

[462] Idem, p. 11-12.
[463] Idem, p. 14. Vgl. ook Reactie T-Mobile op vordering van 21 februari 2013, p. 3-4.
[464] Reactie T-Mobile op vordering van 21 februari 2013, p. 4 Zie ook idem, p. 5 over het gebruik van data-analyse oplossingen: *"De gegevens over en/of uit het mobiele dataverkeer van individuele klanten worden door T-Mobile en met behulp van haar huidige data-analyse oplossingen onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen geanonimiseerd of zodanig geaggregeerd dat deze niet met individuele klanten in verband kunnen worden gebracht."*
[465] Zienswijze 2 T-Mobile, p. 14.
[466] Idem.

op systemen, van waaruit acties worden genomen om te kunnen beschikken over een voldoende capaciteit (uitbreiden, beter verdelen of verplaatsen). Onder 'netwerkbeheer' valt dan ook het monitoren van de alarmen/performance van de verschillende systemen en de verbindingen daartussen. De activiteiten die daarbij horen betreffen [VERTROUWELIJK].[467] T-Mobile voegt in haar reactie op de vordering van het CBP daaraan toe dat zij onder het door haarzelf als zodanig aangeduide doeleinde 'netwerkbeheer en het waarborgen van de integriteit van haar netwerk' verstaat: *"het monitoren van haar (radio)netwerk en services ten aanzien van de beschikbaarheid en kwaliteit van de dienstverlening ter voorkoming van o.m. congestie en netwerkinterrupties."*[468]

Connectiviteit op het netwerk/handset performance voor service management en bewaking van service levels

Onder verwijzing naar haar zienswijze 1 merkt T-Mobile op dat de gegevensverwerkingen ten behoeve van het monitoren en beheren van de connectiviteit van haar netwerk, daaronder mede begrepen de handset performance en bewaking van service levels, geen betrekking hebben op het mobiele internetverkeer (packets) in haar netwerk, maar op het radionetwerk (RAN en UTRAN). Voor deze gegevensverwerkingen wordt geen gebruik gemaakt van deep packet inspection technologie en technieken (door het CBP gedefinieerd als technieken waarmee gegevens uit en over het mobiele internetverkeer kunnen worden geanalyseerd), benadrukt T-Mobile. Deze gegevensverwerkingen vallen daarom buiten het doel van het handhavingsverzoek.[469] In haar reactie op de vordering van het CBP licht T-Mobile toe dat dit feitelijk gebeurt door op verschillende plaatsen in het (radio)netwerk informatie te verzamelen over de activiteit op het netwerk. Deze informatie stelt T-Mobile in staat bijvoorbeeld te zien hoeveel pogingen een handset heeft gedaan voordat hij connectiviteit met het netwerk had, maar ook [VERTROUWELIJK].[470]

Voor zover het CBP, onder verwijzing naar de instellingen van de door T-Mobile gebruikte apparatuur, de antwoorden van T-Mobile op de inlichtingenverzoeken van het CBP en OPTA (die zijn gecontroleerd aan de hand van de bijbehorende (product)documentatie) en het onderzoek ter plaatse van 17 oktober 2011, heeft gemotiveerd dat er wel sprake is van het analyseren en inspecteren van IP-packets, meent T-Mobile dat er sprake lijkt van een misverstand over de werking van haar netwerk. Als verklaring daarvoor noemt T-Mobile dat het CBP, in elk geval toen het feitenonderzoek werd gedaan, wellicht *"niet beschikte over de voldoende kennis over het netwerk van T-Mobile en de wijze waarop daarin het radionetwerk wordt gemonitoord."*[471]

Voor zover het CBP in het kader van dit onderzoek wel in redelijkheid een oordeel zou kunnen geven over deze gegevensverwerkingen, merkt T-Mobile op dat haar abonnees, en die van service-aanbieders die via haar netwerk diensten aan hun eigen abonnees aanbieden, van haar verwachten en contractueel verlangen dat zij zich voortdurend inspant om de diensten zonder onderbreking te verlenen. T-Mobile stelt

[467] Idem.
[468] Reactie T-Mobile op vordering van 21 februari 2013, p. 3.
[469] Zienswijze 2 T-Mobile, p. 15.
[470] Reactie T-Mobile op vordering van 21 februari 2013, p. 7.
[471] Zienswijze 2 T-Mobile, p. 15.

zich op het standpunt dat in een context waarin de omvang en intensiteit van de vraag naar mobiele diensten steeds minder goed voorspelbaar wordt en er sprake is van een exponentiële toename van het gebruik op het signaleringskanaal, dit betekent dat continu moet worden bijgehouden in hoeverre (en waar, met welke frequentie etc.) de pogingen om verbinding te maken met haar netwerk wel of niet succesvol zijn.[472]

T-Mobile verzet zich in haar zienswijze 2 ertegen dat uit de aangehaalde overweging 29 van de e-Privacyrichtlijn zou kunnen worden afgeleid dat voor het meer algemene doel verkeersbeheer verwerking slechts in geaggregeerde vorm zou zijn toegelaten. Dit in verband met het lex certa-en verdedigingsbeginsel én omdat de verwerking voor connectiviteit, handset performance voor service management en bewaking van service levels volgens T-Mobile zonder meer valt onder het 'opsporen van technische defecten en fouten in de transmissie' (overweging 29 van de e-Privacyrichtlijn).[473]

Informatieplicht
Ten eerste betoogt T-Mobile in haar zienswijze 2 dat de gegevens waarop het onderzoek geacht moet worden betrekking te hebben bij de betrokkene zelf worden verkregen. Om die reden kan volgens T-Mobile geen sprake zijn van overtreding van het bepaalde in artikel 34 van de Wbp.[474]

Ten tweede vallen de (niet door T-Mobile, maar door het CBP geformuleerde) 'subdoeleinden' onder de doeleinden die aan de abonnees zijn medegedeeld (T-Mobile verwijst naar paragraaf 3.2 van het Privacy Statement van T-Mobile (versie april 2011) en artikel 12.2 van de Algemene Voorwaarden T-Mobile Consument (versie vanaf 2010). Om de kwaliteit van de dienstverlening te waarborgen worden ook maatregelen genomen om congestie te voorkomen, om netwerkcapaciteit goed te plannen, om virussen en malware te bestrijden en om videoverkeer door middel van compressietechnieken op een voor gebruikers vriendelijke wijze mogelijk te maken, aldus T-Mobile. De wet biedt geen basis om te zeggen dat verantwoordelijken zijn gehouden om betrokkenen te informeren over ieder denkbaar 'subdoel'. Noch uit de vage norm 'wat nodig is om tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen' noch uit artikel 11, eerste lid, onder c, van de Privacyrichtlijn kan worden afgeleid dat T-Mobile gehouden is om de door het CBP (niet T-Mobile) gedefinieerde 'subdoeleinden' bekend te maken aan haar abonnees.[475] T-Mobile begrijpt niet waarom het CBP van mening is dat met het nieuwe Privacy Statement (versie april 2012) een aantal vermeende overtredingen van de informatieplicht is weggevallen, nu T-Mobile vóór de introductie van haar nieuwe Privacy Statement al via de algemene voorwaarden informeerde over deze doeleinden.[476]

Meldingsplicht
T-Mobile gaat er vanuit dat de gestelde overtredingen van de meldplicht overeenkomen met de gestelde overtredingen van de informatieplicht. T-Mobile schrijft daarover dat het CBP daarmee de schijn op zich laadt dat het via de omweg

[472] Idem. Zie ook de Annex bij deze zienswijze.
[473] Idem, p. 16.
[474] Idem, p. 17.
[475] Idem, p. 18. Zie ook idem, p. 22.
[476] Idem, p. 19.

van de meldplicht voor zichzelf de mogelijkheid wil creëren om gebruik te maken van sanctiebevoegdheden bij het toezicht op de naleving van andere verplichtingen dan die waarvoor deze bevoegdheden zijn bedoeld. Dit is in strijd met het verbod van détournement de pouvoir en het legaliteitsbeginsel.[477]

Onder verwijzing naar haar zienswijze 1 betwist T-Mobile dat er een overtreding van de meldplicht is, onder andere door te wijzen op de periode die artikel 28, derde lid, van de Wbp biedt voor het wijzigen van meldingen. Het tijdstip waarop de meldingen zijn gedaan en wanneer deze zijn gewijzigd, toont volgens T-Mobile niet aan en maakt evenmin aannemelijk, dat de wijzigingen niet tijdig zouden zijn gedaan. In dat verband wijst T-Mobile erop dat, mede gelet op de onschuldpresumptie en het zorgvuldigheidsbeginsel, de bewijslast van een overtreding bij het CBP ligt.[478]

Verder meent T-Mobile dat de in de melding m1070767 (versienummer 5.0) genoemde doeleinden 'uitvoering van de overeenkomst' en 'het analyseren van het gebruik van het netwerk' mede betrekking hebben op 'netwerkbeheer, netwerkintegriteit, optimalisatie van de dienstverlening en troubleshooting'. Om die reden is en was de melding toereikend. Voor het overige bedient het CBP zich volgens T-Mobile van een doelredenering gebaseerd op een geconstrueerd en gezocht verschil van inzicht over de betekenis van de in de verschillende meldingen gebruikte begrippen (T-Mobile verwijst ook naar haar zienswijze 1).[479]

Consistentie terminologie én opbouw, structuur en argumentatie van het rapport Reactie CBP: T-Mobile betoogt in haar zienswijze 2 opmerkingen dat het Conceptrapport definitieve bevindingen volgens haar inconsistent is qua terminologie en opzet en structuur, doordat feiten, juridisch kader en beoordeling door elkaar lopen.

Naar aanleiding van de zienswijze 2 van T-Mobile is het toepasselijke en toegepaste wettelijk kader op het punt van de samenloop van Wbp en Tw van Hoofdstuk 1 (Inleiding) naar Hoofdstuk 3 (Uitwerking van het wettelijk kader en beoordeling) verplaatst.

Er is geen wettelijk voorschrift of algemeen rechtsbeginsel dat meebrengt dat Hoofdstuk 2 (Feitelijke bevindingen) geen gedefinieerde termen mag bevatten (bijvoorbeeld 'packet inspection', 'data-analysetechnieken' en gegevens 'over' en 'uit' het dataverkeer) en evenmin dat Hoofdstuk 3 van het rapport niet het wettelijk kader én de beoordeling kan bevatten, per aspect, na elkaar.

Het CBP bestrijdt dat er sprake is van een one-size-fits-all benadering die geen recht doet aan de concrete en specifieke omstandigheden van T-Mobile. Het CBP heeft kennis vergaard over zowel de werkwijze van T-Mobile bij de inzet van data-analysetechnieken, de noodzaak daartoe (bijvoorbeeld op het punt van de netwerkbelasting en de verwachte toename daarvan) en mogelijke alternatieven. Deze concrete en objectieve gegevens zijn aan het rapport ten grondslag gelegd. De

[477] Idem.
[478] Idem, p. 20.
[479] Idem. Zie ook idem, p. 17 e.v. en 22.

zienswijze 2 van T-Mobile heeft op dit punt wel geleid tot aanvulling en verduidelijking van de weerslag van de bevindingen in het rapport.

Ten slotte is de zakelijke inhoud van de zienswijze 1 (zoals in eerste instantie weergegeven in het Conceptrapport definitieve bevindingen) en 2 van T-Mobile, met de reactie daarop van het CBP, opgenomen in twee afzonderlijke bijlagen. Daarbij is de zienswijze 1 gegroepeerd per onderwerp en is aangevuld en verduidelijkt of de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies.

De zienswijze 2 van T-Mobile heeft op dit punt voor het overige niet geleid tot aanpassing van het rapport.

Passende beveiliging van de gegevens
Voor zover T-Mobile in haar zienswijze 2 opmerkt dat de enkele stelling dat een passende beveiliging van de gegevens niet mogelijk zou zijn op gespannen voet staat met artikel 13 van de Wbp en artikel 11.3 van de Tw en áls er is voorzien in een passende beveiliging, de verzameling en verwerking niet om die reden als strijdig met artikel 7 of 8 van de Wbp kan worden gekwalificeerd, wijst het CBP op het volgende.

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). Bij de wijze waarop bepaald wordt wat een passend beveiligingsniveau is, wordt aangesloten bij artikel 13 van de Wbp.[480] De term "passend" duidt blijkens de wetsgeschiedenis bij artikel 13 van de Wbp mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Dat een inbreuk is gemaakt op de beveiliging betekent echter niet per definitie dat de beveiliging, achteraf gezien, niet passend was in de zin van artikel 13 Wbp. De beveiliging moet 'adequaat' zijn.[481] Gelet daarop staat de ervaringsregel van de toezichthouder dat de praktijk leert dat ondanks (passende) technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, (beveiligings)incidenten niet altijd kunnen worden voorkomen niet op gespannen voet met artikel 13 van de Wbp of artikel 11.3 van de Tw.

Zoals vermeld, moet in het kader van de toets van de verwerkingsgrondslag worden nagegaan of (ook) het bewaren en verwerken van de gegevens in niet-geanonimiseerde vorm voldoet aan het proportionaliteits- en subsidiariteitsvereiste.

---

[480] *Kamerstukken II* 2010/11, 32 549, nr. 7, p. 42. Zie ook *T&C Telecommunicatierecht*, commentaar op artikel 11.3 Telecommunicatiewet
[481] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 99 en CBP Richtsnoeren beveiliging van persoonsgegevens van februari 2013, p. 10. URL: http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf (URL laatst bezocht op 29 mei 2013). Zie ook *Kluwer Burgerzaken*, artikel 13 WBP, aantekening 1.3.

Onder andere 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, speelt een rol in die belangenafweging. Anders dan T-Mobile meent, is ten aanzien van de impact (gevolgen van de verdere verwerking voor de betrokkene) onder andere van belang de aard van de betreffende gegevens. Wat betreft de kans is onder meer van belang de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen én de bewaartermijn.

De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Hof van Justitie-arrest Huber
Waar T-Mobile in haar zienswijze 2 de relevantie van het Hof van Justitie-arrest Huber betwist, benadrukt het CBP de betekenis hiervan. Ten eerste vanwege de overweging dat het begrip "noodzakelijkheid" een autonoom begrip van gemeenschapsrecht is en dus niet een inhoud kan hebben die verschilt van lidstaat tot lidstaat.[482] Ten tweede omdat uit het arrest de volgende algemene regel kan worden afgeleid: dat indien het doel de vergaring van statistische gegevens is, het niet noodzakelijk is de persoonsgegevens op naam te bewaren en te verwerken.[483] T-Mobile geeft onder andere in haar zienswijze 2 aan dat zij *"géén gegevens* [verzamelt, toevoeging door het CBP] *op basis van een wettelijke bevoegdheid tot statistische gegevensverwerking, maar (o.a.) omdat zij deze gegevens nodig heeft voor het netwerkbeheer en netwerkintegriteit, waaronder mede begrepen het waarborgen van de veiligheid van haar netwerk, het oplossen en voorkomen van netwerkproblemen, het voorkomen van congestie door forecasting, enz. Deze gegevens worden vervolgens door haar geanonimiseerd en geaggregeerd. Op basis van de geaggregeerde gegevens worden vervolgens niet tot individuele gebruikers herleidbare statistieken samengesteld."*[484] Om zulke trends te berekenen is statistische analyse nodig.

De zienswijze 2 van T-Mobile heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Grondslag netwerkplanning en -beheer
T-Mobile stelt zich in haar zienswijze 2 op het standpunt dat er geen andere, minder ingrijpende middelen zijn om het zelfde resultaat te bereiken, althans dat niet van haar kan worden verlangd dat zij andere middelen implementeert.

---

[482] Vgl. ook HvJ EG 16 december 2008, *EHRC* 2009, 23 (*LJN* BG7811; Huber), r.o. 52.
[483] 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 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."*
[484] Zie o.a. Zienswijze 2 T-Mobile, p. 9.

De zienswijze 2 van T-Mobile heeft op dit punt geleid tot aanvulling en aanpassing van de feitelijke bevindingen, maar met de volgende kanttekeningen: het CBP heeft vastgesteld dat de geaggregeerde data verzameld via de [VERTROUWELIJK: apparatuur] nog e-mailadressen respectievelijk het verbruikte datavolume per top subscriber met MSISDN (heavy user abonnee) bevat (zie hierover verder p. 74 e.v. van dit rapport). T-Mobile heeft dit niet, althans onvoldoende onderbouwd weersproken. T-Mobile heeft met haar zienswijze 2 evenmin als met haar zienswijze 1 op dit punt aldus géén gerede twijfel opgewekt over de juistheid van de feitelijke stelling van het CBP dat er in algemene zin alternatieve maatregelen zijn die kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is.

Wat betreft de inspanning en kosten die voor T-Mobile gepaard gaan met de ontwikkeling en implementatie van een alternatieve oplossing, evenals de consequenties voor de continuïteit en integriteit van haar netwerk, geldt - ten eerste - dat T-Mobile ondanks de vordering van het CBP daartoe geen inschatting heeft gegeven van de kosten (in euro's) en de tijd die het kost (in kalenderdagen) om voor het 'subdoeleinde' van verkeersbeheer (een) data-analyse oplossing(e) te (laten) ontwikkelen, implementeren en beheren die T-Mobile in staat zou stellen om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen te anonimiseren of zodanig te aggregeren dat deze niet met individuele klanten in verband kunnen worden gebracht dan wel om de verwerking van niet-geanonimiseerde gegevens te beperken tot die klanten die daarvoor hun (ondubbelzinnige) toestemming hebben gegeven. Waar T-Mobile in haar zienswijze 2 wel heeft genoemd dat alleen al de kosten van de *vervanging* van de in gebruik zijnde [VERTROUWELIJK: apparatuur]-apparatuur door andere (T-Mobile niet bekende of beschikbare) apparatuur moet worden [VERTROUWELIJK], neemt het CBP - ten tweede - mede in aanmerking dat T-Mobile mogelijk een beroep kan doen op de 'garantie' in de contractsdocumentatie van de [VERTROUWELIJK: apparatuur] dat de producten en diensten voldoen aan de geldende wettelijke normen.[485] Het CBP heeft T-Mobile bevraagd over de nadelige consequenties van het niet zo lang in niet-geanonimiseerde vorm mogen verwerken van de persoonsgegevens. Het is aan de belanghebbende om aan de hand van bijzondere feiten en omstandigheden de schending van het evenredigheidsbeginsel aannemelijk te maken.

Grondslag monitoren en beheren van de connectiviteit van haar netwerk, daaronder mede begrepen de handset performance en bewaking van service levels
T-Mobile stelt zich in haar zienswijze 2 op het standpunt dat omdat voor deze gegevensverwerkingen geen gebruik wordt gemaakt van deep packet inspection technologie en technieken (door het CBP gedefinieerd als technieken waarmee gegevens uit en over het mobiele internetverkeer kunnen worden geanalyseerd), deze gegevensverwerkingen buiten het doel van het handhavingsverzoek vallen. Daarnaast stelt T-Mobile dat omdat netwerkproblemen kunnen worden veroorzaakt door enkele gebruikers, en in voorkomende gevallen alleen kunnen worden opgelost door deze individueel te benaderen, daarvoor niet kan worden volstaan met de verwerking van geanonimiseerde gegeven.

Zoals hierboven gemotiveerd onder het kopje 'Scope: onduidelijkheid omtrent de reikwijdte en het onderwerp van onderzoek' gaat het in dit onderzoek om de wijze

[485] [VERTROUWELIJK]

waarop T-Mobile in haar mobiele netwerk packet inspection technologie en technieken (in het rapport gedefinieerd als data-analysetechnieken) toepast. Onder data-analysetechnieken moet niet alleen worden verstaan *deep* packet inspection. De [VERTROUWELIJK: apparatuur] is geplaatst in het packet geschakelde core netwerk van T-Mobile (zie **bijlage I**). De omstandigheid dat hoeveel pogingen een handset heeft gedaan voordat hij connectiviteit met het netwerk had (vooral) betrekking heeft op het radionetwerk maakt niet dat de gegevensverwerking buiten de scope van dit onderzoek valt. Dit is ook in lijn met de eerdere reactie van T-Mobile op inlichtingenverzoeken van OPTA en het CBP dat de [VERTROUWELIJK: apparatuur] een applicatie is waarmee datapakketten worden geanalyseerd.[486] Het past bovendien in de context van de reden voor data-analyse in mobiele netwerken die T-Mobile noemt: juist 'in een context waarin de omvang en intensiteit van de vraag naar mobiele diensten steeds minder goed voorspelbaar wordt en er sprake is van een exponentiële toename van het gebruik op het signaleringskanaal' vanwege de introductie van smartphones en de komst van chatty apps, moet continu worden bijgehouden in hoeverre (en waar, met welke frequentie etc.) de pogingen om verbinding te maken met haar netwerk wel of niet succesvol zijn.

De zienswijze 2 van T-Mobile heeft op het punt van de noodzaak om via de [VERTROUWELIJK: apparatuur] inzicht te hebben in het netwerkgebruik van individuele eindgebruikers om problemen op te lossen, geleid tot aanvulling en aanpassing van de feitelijke bevindingen en conclusies in het rapport, mede gelet op de verkorting van de bewaartermijnen van de persoonsgegevens.

Informatieplicht
Ten eerste betoogt T-Mobile in haar zienswijze 2 dat de gegevens waarop het onderzoek geacht moet worden betrekking te hebben bij de betrokkene zelf worden verkregen. Om die reden kan volgens T-Mobile geen sprake zijn van overtreding van het bepaalde in artikel 34 van de Wbp. Ten tweede vallen de (niet door T-Mobile, maar door het CBP geformuleerde) 'subdoeleinden' onder de doeleinden die al aan de abonnees zijn medegedeeld.

In de wetsgeschiedenis bij artikel 33 en 34 van de Wbp wordt opgemerkt over het toepassingsbereik van artikel 34: *"Artikel 34 regelt de situatie dat de gegevens op een andere wijze worden verkregen, dus buiten de betrokkene om, hetzij bij derden, bijvoorbeeld gegevens omtrent iemands kredietwaardigheid bij een handelsinformatiebureau, hetzij door eigen observatie, bij voorbeeld naar aanleiding van het gebruik van een netwerk in beheer van de verantwoordelijke"*, (onderstreping toegevoegd door het CBP).[487] De gegevens waarop het onderzoek betrekking heeft, over en uit het mobiel dataverkeer van T-Mobile abonnees, worden daarom verkregen op een andere wijze dan bij de betrokkene, te weten: via het gebruik van data-analysetechnieken in haar mobiele netwerk.

[486] Zie o.a. Reactie T-Mobile op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2 en bijlage 1 bij deze reactie; Reactie T-Mobile op verzoek om inlichtingen van 8 september 2011, p. 3; Reactie T-Mobile op verzoek om inlichtingen van 19 september 2011, p. 2 (op de vraag naar de bewaartermijn van gegevens in, dan wel afkomstig uit de packet inspection apparatuur). En bijlage 1 bij deze reactie.
[487] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149-150.

Uit de wetsgeschiedenis bij de Wbp volgt dat de ratio van de informatieverplichting is dat betrokkene in staat wordt gesteld te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.[488] De informatie moet de betrokkene voldoende houvast bieden om te kunnen voorzien wat er met zijn gegevens gebeurt.[489]

De zinsnede in het oude Privacy Statement 'T-Mobile monitoort daarvoor niet jouw individuele gebruik van het netwerk' moet als feitelijk onjuist worden aangemerkt, althans is onvolledig en onvoldoende duidelijk. Het biedt betrokkenen bijvoorbeeld onvoldoende houvast om te kunnen voorzien dat T-Mobile onder andere 'bijhoudt' welke apps, websites en toepassingen haar klanten gebruiken, zodat zij extra capaciteit in kan zetten als dat nodig is, alsmede analyseert welk toestel de betrokkene gebruikt en hoe dit toestel in haar netwerk functioneert, zoals het aantal succesvol opgezette verbindingen.[490] Verder kan T-Mobile niet volstaan met de mededeling dat gegevens (in abstracto) worden verwerkt om de kwaliteit van de dienstverlening te waarborgen: dit is te weinig specifiek. De betrokkene zal adequaat moeten worden geïnformeerd omtrent (in de woorden van de zienswijze 2 van T-Mobile) maatregelen genomen om congestie te voorkomen, om netwerkcapaciteit goed te plannen, om virussen en malware te bestrijden en om videoverkeer door middel van compressietechnieken op een voor gebruikers vriendelijke wijze mogelijk te maken als het concrete doel van de gegevensverwerking als toetsingskader voor zorgvuldig gebruik enz.

De zienswijze 2 van T-Mobile heeft geleid tot aanpassing en verduidelijking in het rapport dat getoetst wordt de informatie over onder andere de door T-Mobile genoemde concrete doelen van de gegevensverwerking). De zienswijze 2 van T-Mobile heeft op het punt van de informatieplicht geleid tot aanpassing en verduidelijking van het toepasselijke en toegepaste wettelijk kader, vanwege de afstemming van de toepassing van dit wetsartikel en artikel 11.5, vierde lid, van de Tw. De zienswijze 2 van T-Mobile heeft niet geleid tot aanpassing van de conclusies in het rapport.

Meldingsplicht
T-Mobile gaat er vanuit dat de gestelde overtredingen van de meldplicht overeenkomen met de gestelde overtredingen van de informatieplicht. T-Mobile betwist dat de gewijzigde wijzigingen niet tijdig zouden zijn gedaan (onder andere onder verwijzing naar de onschuldpresumptie). Ten slotte meent T-Mobile dat de doeleinden van de gegevensverwerking volledig en voldoende duidelijk was omschreven in de doelomschrijving in een van de meldingen die T-Mobile heeft gedaan.

---

[488] Idem, p. 149.
[489] Zie ook *Kamerstukken II* 1998/99, 25 892, nr. 6, p. 17*: "Daar waar normaal commercieel gebruik van persoonsgegevens is toegestaan, zal de betrokkene in beginsel wel op de hoogte moeten worden gesteld van het doel waarvoor de gegevens worden verwerkt. Daarbij kan de verantwoordelijke niet volstaan met de mededeling dat gegevens in abstracto worden verwerkt voor commerciële doeleinden: dit is te weinig specifiek. Het biedt de betrokkene onvoldoende houvast om te kunnen voorzien wat er met zijn gegevens gebeurt. De betrokkene zal adequaat moeten worden geïnformeerd omtrent het concrete doel van de gegevensverwerking als toetsingskader voor zorgvuldig gebruik."*
[490] Vgl. Privacy Statement T-Mobile (versie december 2012).

Anders dan T-Mobile veronderstelt, vloeit de geconstateerde overtreding van de meldingsplicht niet voort uit de overtreding van de informatieplicht. Zowel aanmelding als mededeling dat gegevens worden verwerkt hebben echter tot doel de transparantie van de gegevensverwerking te bevorderen[491]: ze vormen het criterium aan de hand waarvan de omgang met de persoonsgegevens wordt getoetst.[492] Zowel de meldingsplicht als de informatieplicht vereisen bovendien mededeling van de doeleinden van de gegevensverwerking. Dit maakt evenwel niet dat het CBP 'via de omweg van de meldplicht voor zichzelf de mogelijkheid wil creëren om gebruik te maken van sanctiebevoegdheden bij het toezicht op de naleving van andere verplichtingen dan die waarvoor deze bevoegdheden zijn bedoeld'. Zulks volgt ook geenszins uit het rapport.

De te melden gegevens (waaronder het doel of de doeleinden van de verwerking en een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben) zijn duidelijk en precies geformuleerd in artikel 28, eerste lid, van de Wbp. De vraag welke informatie T-Mobile aan de betrokkenen moet verstrekken, kan worden beantwoord aan de hand van de tekst van de wet, de wetsgeschiedenis van artikel 34 van de Wbp[493], de Wbp-naslag van het CBP[494], de CBP Richtsnoeren publicatie van persoonsgegevens op internet[495], met als bijlage een model privacyverklaring en opinies van de Artikel 29-werkgroep.[496]

Zoals hierboven gemotiveerd, is van een criminal charge in dit onderzoek geen sprake. Er geldt daarom geen 'onschuldpresumptie' (zie p. 117 van dit rapport).

Wat betreft de procedure wijzingen aan te brengen in de melding wordt in de wetsgeschiedenis bij artikel 28 van de Wbp opgemerkt: "*Het derde lid geeft invulling aan de opdracht van artikel 19, tweede lid van de richtlijn, namelijk dat een procedure moet worden voorgeschreven voor het melden van wijzigingen. (…) In het derde lid is tevens, teneinde de administratieve belasting zoveel mogelijk te verminderen, neergelegd dat wijzigingen in de overige gegevens slechts behoeven te worden gemeld, indien na verloop van tijd blijkt dat deze van meer dan incidentele aard zijn. De gegevensverwerking dient eens per jaar daarop te*

[491] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 132 en 149.
[492] Zie ook *Kamerstukken II* 1998/99, 25 892, nr. 6, p. 17 en *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 136.
[493] Zie o.a. idem, p. 149-157.
[494] URL: http://www.cbpweb.nl/wbpnaslag/5/Paginas/Wbp-hoofdstuk-5-informatieverstrekking-aan-de-betrokkene.aspx (URL laatst bezocht op 29 mei 2013).
[495] CBP Richtsnoerenpublicatie van persoonsgegevens op internet van december 2007, p. 25-28. URL: http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf (URL laatst bezocht op 29 mei 2013).
[496] WP29 203. Opinion 03/2013 on purpose limitation, dated 2 April 2013. WP29 100. Advies 10/2004 over meer geharmoniseerde bepalingen inzake informatieverstrekking van 25 november 2004, met bijlagen. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_nl.pdf. WP29 43. Recommendation on certain minimum requirements for collecting personal data on-line in the European Union, dated 17 mei 2001. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp43en.pdf (URL's laatst bezocht op 29 mei 2013).

worden gecontroleerd."[497] Het CBP heeft geconcludeerd dat de overtreding van de meldingsplicht ten dele was beëindigd, doordat T-Mobile de doeleinden netwerkbeheer en -integriteit en troubleshooting alsnog had gemeld bij het CBP.

De melding dat gegevens (in abstracto) worden verwerkt voor 'het registreren van gegevens over afgewikkeld verkeer van spraak en data ten behoeve van onderzoek naar hoogverbruik en (intern) fraudeonderzoek', 'het sluiten en uitvoeren van de overeenkomst die het gevolg is van een aansluiting' en 'het analyseren van het gebruik van het netwerk' was onvolledig en onvoldoende duidelijk. De afweging van de belangen van de verantwoordelijke en de betrokkene was zodoende onvoldoende controleerbaar.[498]

De zienswijze 2 van T-Mobile heeft op het punt van de meldingsplicht geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader, evenals de conclusies in het rapport.

Getroffen maatregelen

Zienswijze 2 T-Mobile: Zonder aanvaarding van enige gehoudenheid daartoe heeft T-Mobile haar meldingen eind 2011 gewijzigd (versienummer 6.0). Daardoor kan volgens T-Mobile geen sprake meer zijn van overtredingen. 'Optimalisatie van de dienstverlening aan klanten (waaronder begrepen videocompressie)' zijn (wél) voldoende duidelijk beschreven in de gewijzigde meldingen (onderdeel van de dienstverlening van T-Mobile).[499] T-Mobile heeft (bovendien) haar melding 'netwerkbeheer en gebruikersmanagement' (m1070731) per 30 oktober 2012 (nogmaals) gewijzigd.[500]

Verder heeft T-Mobile haar bedrijfsprocessen nog eens tegen het licht gehouden en is zij inmiddels overgegaan tot het aanpassen van haar bedrijfsprocessen en de informatievoorziening aan haar abonnees en eindgebruikers. In haar Privacy Statement heeft T-Mobile extra informatie opgenomen over de verwerkingen van persoonsgegevens. Op een voor abonnees en eindgebruikers begrijpelijke wijze wordt uiteengezet welke categorieën van persoonsgegevens T-Mobile verzamelt, waarbij een onderverdeling is gemaakt naar gebruikersgegevens, verkeersgegevens en locatiegegevens. Ook wordt toegelicht voor welke doeleinden de persoonsgegevens worden verwerkt, hoe deze worden beveiligd en wordt de betrokkene op zijn rechten onder de Wbp gewezen. Een vernieuwd Privacy Statement (versie december 2012) met nog meer informatie is inmiddels bekendgemaakt.[501] Ten slotte heeft T-Mobile de

[497] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 139.
[498] Idem, p. 132-133: *"Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn."*
[499] Zienswijze 2 T-Mobile, p. 20-21. Zie ook idem, p. 22.
[500] E-mail T-Mobile van 21 december 2012.
[501] Idem, p. 22. Zie ook e-mail T-Mobile van 21 december 2012.

bewaartermijnen van de geaggregeerde gegevens via de [VERTROUWELIJK: apparatuur] verkort tot:

- 15 dagen (op 15 minuten basis geaggregeerde data);
- 15 dagen (op dagbasis geaggregeerde data); en
- 14 dagen (op weekbasis geaggregeerde data).[502]

Het CBP leidt uit de reactie van T-Mobile op de vordering af dat er geen op maandbasis geaggregeerde data meer wordt bewaard.[503]

Reactie CBP: Doordat T-Mobile 'optimalisatie van de dienstverlening aan klanten (waaronder begrepen videcompressie' alsnog heeft omschreven in de melding met nummer m10700731, handelt T-Mobile niet langer in strijd met de meldingsplicht.

Doordat T-Mobile als concrete doelen van de gegevensverwerking heeft medegedeeld in haar nieuwste Privacy Statement (versie december 2012): analyse van welk toestel de betrokkene gebruikt en hoe dit toestel in haar netwerk functioneert, zoals het aantal succesvol opgezette verbindingen; maatregelen genomen om congestie te voorkomen; om netwerkcapaciteit goed te plannen; om virussen en malware te bestrijden en om videoverkeer door middel van compressietechnieken op een voor gebruikers vriendelijke wijze mogelijk te maken, handelt T-Mobile in dit verband in zoverre niet langer in strijd met de meldingsplicht. De geconstateerde overtredingen duren voort op het gebied van het (gedeeltelijk) ontbreken van informatie aan abonnees over de duur van de verwerking (bewaartermijnen).

Doordat T-Mobile voor het detecteren en oplossen van problemen in het netwerk via de [VERTROUWELIJK: apparatuur] de persoonsgegevens - als gevolg van het verkorten van de bewaartermijnen - de persoonsgegevens inmiddels zo snel als mogelijk na het verzamelen verwijdert, heeft zij in dit verband in zoverre een grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Op deze punten is T-Mobile niet langer in overtreding (grondslag).

De zienwijze 2 van T-Mobile heeft op deze punten geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies.

[502] Reactie T-Mobile op vordering van 21 februari 2013, p. 7-8.
[503] Idem.