

College bescherming persoonsgegevens

Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Tele2 Nederland B.V.

Z2011-00462

Rapport definitieve bevindingen
Mei 2013 met corrigendum van 12 juni 2013

OPENBARE VERSIE

Inhoudsopgave

Inhoudsopgave.....	1
Samenvatting.....	2
1. Inleiding.....	5
2. Feitelijke Bevindingen.....	13
2.1 Organisatiebeschrijving	13
2.2 Mobiel netwerk, netwerkverkeer en plaatsing data-analyse apparatuur.....	15
2.3 Doeleinden.....	18
2.4 Netwerkbeheer en marktonderzoeksdoeleinden.....	19
2.5 Prepaidverkeer.....	28
2.6 Spam-, virus- en spywarefiltering van e-mailverkeer	29
3. Uitwerking van het wettelijk kader en beoordeling.....	32
3.1 Wettelijk kader: samenloop Wbp en Tw	32
3.2 Verantwoordelijke	33
3.3 Verwerking van persoonsgegevens	34
3.4 Verkeersgegevens versus communicatie	46
3.5 Gegevensverwerking	50
3.6 Grondslag	51
3.6.1 Netwerkbeheer en marktonderzoeksdoeleinden.....	64
3.6.2 Prepaidverkeer.....	68
3.6.3 Spam-, virus- en spywarefiltering van e-mailverkeer	70
3.7 Uitdrukkelijk omschreven en gerechtvaardigde doeleinden.....	72
3.8 Informatieplicht	74
3.9 Meldingsplicht	79
3.10 Bewerkersovereenkomst.....	81
3.11 Doorgifte	84
4. Conclusie	87

Bijlagen:

- I. Schema mobiel netwerk Tele2
- II. Verklarende woordenlijst
- III. Zienswijze 1 van Tele2, met de reactie daarop van het CBP
- IV. Zienswijze 2 van Tele2, met de reactie daarop van het CBP

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar de wijze waarop Tele2 *packet inspection* technologie en technieken (hierna: data-analyse technieken) toepast in het mobiele netwerk van het bedrijf. Onder data-analyse technieken wordt verstaan: technieken waarmee gegevens over en uit het mobiele dataverkeer kunnen worden geïnspecteerd en geanalyseerd. Het CBP heeft onderzocht of Tele2 hierbij persoonsgegevens verwerkt en zo ja, of Tele2 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 Tele2

Tele2 verwerkt gegevens over en uit het dataverkeer van naar schatting 250.000 Tele2-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.

Tele2 verwerkt de persoonsgegevens voor het doeleinde van netwerkbeheer en marktonderzoek en ten behoeve van spam, virus- en spywarebestrijding in het e-mailverkeer.

Om websites, apps en protocollen te herkennen, inspecteert en analyseert Tele2 gegevens over het dataverkeer [VERTROUWELIJK]. De gegevens over het dataverkeer kunnen inhoudskenmerken bevatten, zoals informatie over bezochte websites en gebruikte apps. Dat soort gegevens zijn ‘gevoelige’ persoonsgegevens. Teneinde spam en virussen en spyware te filteren, inspecteert en analyseert Tele2 de inhoud van e-mailverkeer. Dat soort gegevens zijn communicatiegegevens.

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Eén van die eisen is dat er een rechtvaardigingsgrond (grondslag) moet zijn voor de verwerking. Het CBP heeft bij Tele2 gedurende het onderzoek een aantal overtredingen van de Wbp en de Tw geconstateerd.

Netwerkbeheer en marktonderzoek

Het verwerken van persoonsgegevens voor het doeleinde netwerkbeheer is alleen toegestaan als de persoonsgegevens zo snel mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren. Hoewel Tele2

[VERTROUWELIJK: identifier] versleutelt en andere identificerende gegevens alleen gedurende de internet sessie van een abonnee vastlegt, leidt de toegepaste versleuteling niet tot onomkeerbare anonimisering. De verzamelde gegevens blijven daardoor persoonsgegevens. Omdat de huidige werkwijze van Tele2 voor het doeleinde van netwerkbeheer niet voldoet aan de vereisten van proportionaliteit en subsidiariteit is van een noodzaak voor het gebruiken, vastleggen en bewaren van persoonsgegevens geen sprake. Omdat Tele2 ook geen ander noodzakelijk verwerkingsdoeleinde heeft voor deze gegevensverwerking, is Tele2 hierdoor in overtreding.

Verder mogen deze gegevens niet zonder ondubbelzinnige toestemming van de abonnees worden verwerkt voor marktonderzoek. Omdat Tele2 de (versleutelde) gegevens wel voor marktonderzoeksdoeleinden gebruikt, is Tele2 hierdoor in overtreding.

Meldingsplicht

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen wettelijk verplicht deze gegevensverwerking te melden bij het CBP. De meldingen van Tele2 bevatten echter onvoldoende duidelijke informatie over de doeleinden waarvoor Tele2 persoonsgegevens verwerkt. Tele2 is hierdoor in overtreding.

Bewerkersovereenkomst

Op grond van de Wbp is een bedrijf verplicht een bewerkersovereenkomst te sluiten als een ander ten behoeve van het bedrijf persoonsgegevens verwerkt. Tele2 is in overtreding omdat Tele2 geen bewerkersovereenkomsten heeft gesloten met [VERTROUWELIJK: A] en met [VERTROUWELIJK: B].

Internationale gegevensverstrekking

Doorgifte van persoonsgegevens naar een land buiten de Europese Unie is alleen toegestaan als dit land een passend beschermingsniveau biedt. In geval van onderhoud en/of storing biedt Tele2 toegang tot de persoonsgegevens aan [VERTROUWELIJK: A] in twee landen die dit niveau niet bieden: [VERTROUWELIJK]. Tele2 is hierdoor in overtreding.

Overtredingen die gedeeltelijk zijn beëindigd

Informeren abonnees

Tele2 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. Tele2 informeerde abonnees onvoldoende over de soorten persoonsgegevens die zij met de toepassing van data-analysetechnieken verkrijgt voor het doeleinde netwerkbeheer en marktonderzoek. Daarnaast informeerde Tele2 hen niet over de bewaartermijn van de verschillende gegevens. Tele2 was hierdoor in overtreding.

Tele2 heeft in april 2013 voor het eerst een (algemeen) Privacy Statement gepubliceerd. Door deze getroffen maatregel zijn de geconstateerde overtredingen gedeeltelijk beëindigd. De overtreding van de informatieplicht duurt voort op het gebied van het ontbreken van informatie aan abonnees over de duur van de verwerking (bewaartermijnen) en over het doeleinde van de verwerking voor marktonderzoeksdoeleinden.

Geen overtredingen

Spam- virus- en spywarebestrijding e-mail verkeer

Tele2 heeft een wettelijke grondslag voor de verwerking ten behoeve van spam-, virus- en spywarebestrijding in het e-mailverkeer. Op dit punt is Tele2 dan ook niet in overtreding (geweest).

Prepaid verkeer

Tot april 2012 verwerkte Tele2 ook persoonsgegevens om het bezoek aan en gebruik van (gratis) opwaardeersites te faciliteren van prepaid-abonnees bij een ontoereikend tegoed. Omdat Tele2 [VERTROUWELIJK] en geen gegevens bewaarde, was de werkwijze proportioneel. Tele2 was hierdoor niet in overtreding.

Voorgestelde maatregelen

Tele2 heeft twee alternatieve wijzigingen voorgesteld van de wijze van versleuteling van de [VERTROUWELIJK: identifier]. Toepassing van deze methodes leidt echter niet tot de conclusie dat geen sprake meer is van persoonsgegevens.

Tele2 heeft concept wijzigingen en aanvullingen gestuurd op de melding bij het CBP en het Privacy Statement van het bedrijf. Deze maatregelen leiden echter, ook na daadwerkelijke invoering ervan, (nog) niet tot beëindiging van de geconstateerde overtredingen van de informatie- en meldplicht.

Tele2 heeft tevens [VERTROUWELIJK] conceptovereenkomsten toegestuurd om de geconstateerde overtredingen te beëindigen ten aanzien van (het inschakelen van) bewerkers en internationale doorgifte van persoonsgegevens.

De overtreding ten aanzien van internationale doorgifte wordt beëindigd als partijen de voorgelegde concept-doorgifteovereenkomst ondertekenen. Aangaan van de bewerkersovereenkomsten leidt onder voorwaarden tot beëindiging van de overtreding.

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 Tele2 Nederland B.V. (hierna: Tele2) in haar mobiele netwerk *packet inspection* technologie en technieken (hierna: data-analyse technieken) toepast.

Het CBP heeft onderzocht of Tele2 hierbij persoonsgegevens verwerkt en zo ja, of Tele2 zich houdt aan de Wbp en hoofdstuk 11 van de Telecommunicatiewet (hierna: Tw).

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

Achtergrond onderzoek

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

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

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

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

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

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

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

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

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

OPTA heeft in mei en juni 2011 onderzoek uitgevoerd onder de vier grootste mobiele netwerkaanbieders in Nederland (KPN, Vodafone, T-Mobile en Tele2) naar de vraag

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

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

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

⁶ Van de totaal 22.098.000 mobiele aansluitingen aan het eind van 2012 in Nederland, waren er 9.063.000 met mobiel breedbandinternet en 1.185 specifieke mobiele breedbandaansluitingen, zoals tablets en dongels. In totaal 10.248.000 mobiele internetaansluitingen, ofwel 46,4 procent van het totaal aantal mobiele aansluitingen. Bron tabel 'Mobiel: Marktaandelen retail aansluitingen' uit de ACM Openbare rapportage mobiel Q4, p. 1, URL: <https://www.acm.nl/nl/download/bijlage/?id=10942> (URL laatst bezocht op 29 mei 2013). Het feitelijke percentage mobiele aansluitingen met data-abonnement verschilt per operator. Vgl. 'Consumenten kopen handset in winkel, bestellen sim online', *Telecompaper* 11 juli 2012. URL: <http://www.telecompaper.com/nieuws/consumenten-kopen-handset-in-winkel-bestellen-sim-online> (URL laatst bezocht op 29 mei 2013). Vgl. ook TNO Marktrapportage Elektronische Communicatie (MEC) eerste helft 2012, 18 februari 2013, URL: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2013-02-18%2016:42:09.0 (URL laatst bezocht op 29 mei 2013).

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

of en zo ja, hoe deze partijen hun dataverkeer analyseren. OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van het Samenwerkingsprotocol CBP-OPTA van 12 juli 2005.

Bevoegdheid CBP

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

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

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

“Op grond van artikel 51 van het voorliggende wetsvoorstel wordt het Cbp belast met het toezicht op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens de wet bepaalde. Dit betekent dat het Cbp een algemene toezichtsbevoegdheid heeft die zich niet alleen uitstrekt tot de naleving van het bij of krachtens het voorstel voor een Wet bescherming persoonsgegevens bepaalde, maar ook tot hetgeen bij of krachtens hoofdstuk 11 van het voorstel voor een Telecommunicatiewet is bepaald, voor zover het de verwerking van persoonsgegevens betreft. (...) De OPTA is ook belast met toezicht op de naleving en de bestuursrechtelijke handhaving van hoofdstuk 11 [van de Tw, toevoeging door het CBP]. Die bevoegdheden zullen met name betekenis hebben voor zover het niet de verwerking van persoonsgegevens betreft.”⁹

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

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

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

⁹ Kamerstukken II 1998/99, 25 892, nr. 6, p. 43. Zie Kamerstukken II 2002/03, 28 851, nr. 3, p. 61: “Het CBP is op grond van de Wbp belast met het toezicht op de naleving van de Wbp in het algemeen, en waar het de verwerking van persoonsgegevens door aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten op grond van hoofdstuk 11 Telecommunicatiewet betreft, ook op die bepalingen. Daarnaast is het college [van OPTA, toevoeging door het CBP] op basis van hoofdstuk 15 Telecommunicatiewet belast met het toezicht op hoofdstuk 11 Telecommunicatiewet als geheel. De nadruk in het toezicht van het college ligt echter op andere aspecten van hoofdstuk 11 Telecommunicatiewet dan die waarop het CBP toeziet.” Zie ook Kamerstukken I 2003/04, 28 851, nr. C, p. 34; Kamerstukken II 2002/03, 28 851, nr. 7, p. 43 en Kamerstukken II 1997/98, 25 533, nr. 5, p. 117.

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

Onderzoeksvragen

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

- Zijn de gegevens over en uit het mobiele dataverkeer die Tele2 verzamelt persoonsgegevens, zoals gedefinieerd in artikel 1, aanhef en onder a, van de Wbp?
- Zijn de doeleinden waarvoor Tele2 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 Tele2 als bedoeld in artikel 8 van de Wbp?
- Heeft Tele2 de betrokkenen (tijdig) geïnformeerd over de gegevensverwerking, zoals bepaald in artikel 34 van de Wbp?
- Heeft Tele2 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?

Het CBP heeft naar aanleiding van de reactie van Tele2 op het eerste inlichtingenverzoek twee aanvullende onderzoeksvragen gesteld:

- Heeft Tele2 (een) bewerkersovereenkomst(en) gesloten als bedoeld in artikel 14 van de Wbp?
- Worden er persoonsgegevens doorgegeven naar (een) land(en) buiten de Europese Unie/Europese Economische Ruimte zonder passend beschermingsniveau als bedoeld in artikel 76 van de Wbp?

Verloop onderzoek

OPTA heeft in mei 2011 onderzoek (een quick scan) ingesteld onder de vier grootste mobiele netwerkaanbieders (KPN, Vodafone, T-Mobile en Tele2) naar de vraag of de

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

manier waarop de mobiele netwerkaanbieders datapakketten analyseren strijdig is met bepalingen uit de Tw.¹¹

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

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

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

Bij brief van 18 augustus 2011 heeft het CBP schriftelijk inlichtingen ingewonnen bij Tele2. Tele2 heeft het CBP bij brief van 24 augustus 2011 verzocht om uitstel van de termijn voor het geven van een reactie met een aantal weken. Het CBP heeft Tele2 bij brief van 25 augustus 2011 uitstel verleend tot en met 15 september 2011. Op 8 september 2011 heeft Tele2 telefonisch nader uitstel verzocht van de termijn voor het geven van een reactie tot en met 19 september 2011. Het CBP heeft Tele2 op 8 september 2011 mondeling het gevraagde nadere uitstel verleend. Tele2 heeft de inlichtingen op 19 september 2011 aan het CBP verstrekt.

Op 20 september 2011 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en [VERTROUWELIJK] Tele2 over het onderzoek.

Bij brief van 19 oktober 2011 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij Tele2. Tele2 heeft bij brief van 24 oktober 2011 verzocht om uitstel van de termijn voor het geven van een reactie tot en met 9 november 2011. Het CBP heeft bij brief van 25 oktober 2011 voor het aanleveren van een deel van de antwoorden uitstel verleend tot en met 2 november 2011 en ten aanzien van de overige vragen tot en met 9 november 2011. Tele2 heeft de gevraagde inlichtingen (zoals gepreciseerd in een e-mail van het CBP van 4 november 2011) op 2 respectievelijk 9 november 2011 gedeeltelijk aan het CBP verstrekt.

Bij brief van 11 november 2011 heeft het CBP Tele2 verzocht de ontbrekende antwoorden en (kopieën van) bescheiden op de inlichtingenverzoeken van 19 oktober respectievelijk 4 november 2011 uiterlijk op 16 november 2011 alsnog aan het CBP te verstrekken. Tele2 heeft bij brief van 15 november 2011 verzocht om uitstel van de termijn voor het geven van deze antwoorden en (kopieën van) bescheiden tot en met 30 november 2011. Het CBP heeft Tele2 bij brief van 16 november 2011 uitstel verleend tot en met 23 november 2011 en Tele2 verzocht de ondertekeningsbevoegdheid van

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

¹² Idem.

[VERTROUWELIJK] van Tele2 aan te tonen. Tele2 heeft de gevraagde volmacht op 21 november 2011 aan het CBP verstrekt. Tele2 heeft de ontbrekende inlichtingen op 23 november 2011 slechts gedeeltelijk aan het CBP verstrekt.

Bij brief van 25 november 2011 heeft het CBP Tele2 verzocht de ontbrekende antwoorden en (kopieën van) bescheiden op de inlichtingenverzoeken van 19 oktober respectievelijk 4 en 11 november 2011 uiterlijk op 30 november respectievelijk 2 december 2011 alsnog aan het CBP te verstrekken. Tele2 heeft de ontbrekende inlichtingen op 30 november respectievelijk 2 december 2011 slechts gedeeltelijk aan het CBP verstrekt.

Op 5 december 2011 heeft het CBP Tele2 een informatievordering gezonden om de ontbrekende inlichtingen uiterlijk op 12 december 2011 aan het CBP te verstrekken. Op 8 december 2011 heeft telefonisch overleg plaatsgevonden tussen een medewerker van het CBP en [VERTROUWELIJK] van Tele2 over het onderzoek. Tele2 heeft bij faxbrief van 12 december 2011 en bij brief van 13 december 2011 (door het CBP ontvangen op 14 december 2011) slechts een deel van de gevorderde inlichtingen verstrekt. Bij brief van 15 december 2011 heeft het CBP een rappel vordering gestuurd aan Tele2, om de ontbrekende inlichtingen uiterlijk op 22 december 2011 aan het CBP te verstrekken. Het CBP heeft daarin aangegeven zijn voornemen te handhaven om over te gaan tot het opleggen van een last indien niet aan de vordering zou worden voldaan. Bij brief van 20 december 2011 heeft Tele2 aan de vordering voldaan.

Het CBP heeft op 12 januari 2012 het rapport voorlopige bevindingen vastgesteld. Het CBP heeft Tele2 bij brief van 13 januari 2012 in de gelegenheid gesteld om haar zienswijze op het rapport voorlopige bevindingen naar voren te brengen. Tele2 heeft bij brief van 9 februari 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 9 maart 2012. Het CBP heeft bij brief van 10 februari 2012 uitstel verleend tot 29 februari 2012. Tele2 heeft haar zienswijze op 29 februari 2012 schriftelijk ingebracht.

Op 23 maart 2012 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij Tele2. Tele2 heeft de gevraagde inlichtingen op 11 april 2012 aan het CBP verstrekt.

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

Op 11 juni 2012 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en [VERTROUWELIJK] van Tele2 over het onderzoek.

Op 3 augustus 2012 heeft het CBP mondeling inlichtingen ingewonnen bij Tele2.

Het CBP heeft op 21 augustus 2012 het conceptrapport definitieve bevindingen vastgesteld. Het CBP heeft Tele2 bij brief van 21 augustus 2012 in de gelegenheid gesteld om haar zienswijze op het conceptrapport definitieve bevindingen uiterlijk 2 oktober 2012 naar voren te brengen. Tele2 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 Tele2 gevraagde uitstel verleend. Tele2 heeft haar zienswijze op 30 oktober 2012 schriftelijk ingebracht.

Bij brief van 12 december 2012 heeft het CBP Tele2 geïnformeerd over de planning van het onderzoek. Bij brief van 19 december 2012 heeft het CBP inlichtingen gevorderd en inzage in zakelijke gegevens en bescheiden. Tele2 heeft bij fax van 24 december 2012 om uitstel van beantwoording gevraagd. Naar aanleiding van een telefonisch verzoek van het CBP op 2 januari 2013 om motivering van het gevraagde uitstel, heeft Tele2 gereageerd per e-mail van 7 januari 2013. Bij brief van 9 januari 2013 heeft het CBP uitstel verleend tot 21 februari 2013. Bij brief van 21 februari 2013 heeft Tele2 gereageerd op de vordering.

Op 15 april 2013 en op 16 mei 2013 heeft het CBP Tele2 telefonisch geïnformeerd over de planning van het onderzoek.

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

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

Zienswijze van Tele2 op de voorlopige bevindingen van het CBP van 12 januari 2012

In haar zienswijze van 29 februari 2012 op het Rapport voorlopige bevindingen van het CBP (hierna: Zienswijze 1), daaronder begrepen de daarop volgende correspondentie, brengt Tele2, samengevat weergegeven, naar voren dat het rapport voorlopige bevindingen onzorgvuldig is voorbereid en ontoereikend is gemotiveerd.

Tele2 betoogt dat de data-analyse in belangrijke mate betrekking heeft op verkeersgegevens in de zin van hoofdstuk 11 van de Tw. Als er (ook) sprake is van persoonsgegevens, is er samenloop van de Wbp met de Tw. Bij invulling van de normen van de Wbp mag het CBP niet voorbijgaan aan de specifieke invulling die daaraan door de (Nederlandse en Europese) wetgever is gegeven voor de telecomsector. Tele2 benadrukt dat netwerkbeheer onder de e-Privacyrichtlijn uitdrukkelijk is erkend als legitiem doel voor de tijdelijke opslag van communicatie- en verkeersgegevens, mits het vertrouwelijke karakter gewaarborgd blijft.

Het CBP moet in zijn beoordeling volgens Tele2 uitgaan van de feitelijke implementatie van de ten behoeve van Tele2 ingezette data-analyse apparatuur en zich niet louter baseren op (algemene) technische documentatie.

Tele2 betwist dat alle door Tele2 verwerkte gegevens moeten worden aangemerkt als persoonsgegevens. Tele2 geeft aan dat zij in de meeste gevallen niet bekend is met de NAW-gegevens van haar prepaid abonnees.

Tele2 wijst erop dat de door het CBP aangedragen alternatieven niet (zonder meer) geschikt zijn. Volgens Tele2 kan zij aan algemene marktmonitors en klantenpanels geen nauwkeurige, statistische informatie ontleen over welk gebruik haar abonnees daadwerkelijk maken van het mobiele netwerk. Tele2 meent dat de Wbp er niet aan in

de weg staat dat data-analyse technologie wordt ingezet om op anonieme basis gebruiksstatistieken te genereren.

Tele2 betwist dat een bewerkersovereenkomst is vereist en dat er sprake zou zijn van doorgifte naar landen buiten de Europese Unie zonder passend beschermingsniveau. Niettemin is zij bereid om met [VERTROUWELIJK: A/B] in overleg te treden over het aangaan van een bewerkers- en doorgifteovereenkomst.

Tele2 geeft aan dat zij de conclusie van het rapport voorlopige bevindingen ernstig heeft opgenomen. Tele2 heeft besloten om toepassing van de onderzochte data-analyse technieken (tijdelijk) op te schorten, uiterlijk met ingang van 11 april 2012, tenzij zij binnen die termijn andere maatregelen kan treffen om de door het CBP gesignaleerde bezwaren weg te nemen, zoals een verzwaring van de versleuteling en het vragen van ondubbelzinnige toestemming aan prepaid abonnees.

Bij brief van 11 april 2012 heeft Tele2 het CBP laten weten dat de data-analyse apparatuur om prepaid abonnees in staat te stellen gratis hun tegoed op te waarderen niet meer wordt gebruikt en dat nadere informatie over de gebruikte versleuteling bij de data-analyse apparatuur die wordt gebruikt voor netwerkbeheer en marktonderzoeksdoeleinden er volgens Tele2 toe leidt dat er geen sprake is van persoonsgegevens.

In **bijlage III** bij dit rapport is de zakelijke inhoud van de zienswijze van Tele2 opgenomen per onderdeel (met de toevoeging '**Zienswijze 1 Tele2**'), 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.

Zienswijze van Tele2 op concept definitieve bevindingen van het CBP van 21 augustus 2012

In haar zienswijze van 30 oktober 2012 op het CBP Conceptrapport definitieve bevindingen (hierna: Zienswijze 2), en latere brief van 21 februari 2013, brengt Tele2 naar voren dat het CBP feitelijke fouten heeft hersteld in het conceptrapport definitieve bevindingen, maar dat de conclusies van het CBP niet wezenlijk veranderd zijn.

Tele2 maakt bezwaar tegen opname van het gebruik van spam-, virus- en spywarefiltering van e-mailverkeer in het rapport, omdat dit volgens haar geen relatie heeft met het onderwerp van het onderzoek, de toepassing van *deep packet inspection* technieken.

Tele2 stelt dat de gebruikte versleuteling van de [VERTROUWELIJK: identifier] ertoe leidt dat de identiteit van de gebruiker niet, of slechts met onevenredige inspanningen, valt te achterhalen. Dit geldt zowel voor het door het CBP geschetste scenario van ontsleuteling door Tele2 zelf, als voor ontsleuteling door de technici van [VERTROUWELIJK: A/B]. Tele2 is niettemin bereid om de afspraken tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: B] aan te vullen, en heeft daartoe conceptafspraken gevoegd als bijlage 1 bij haar zienswijze 2.

Volgens Tele2 is het oordeel van het CBP dat er andere, minder ingrijpende alternatieven zouden bestaan, onjuist. Verwijdering of anonimisering van de persoonsgegevens leidt ertoe dat het niet meer mogelijk is individuele gebruikspatronen van elkaar te onderscheiden. Tele2 betoogt dat het voor netwerkbeheer noodzakelijk is om dataverbruik te kunnen waarnemen op individueel niveau, door de tijd heen, om trends te kunnen waarnemen en te kunnen anticiperen op veranderingen in het dataverkeer over tijd. Deze informatie kan aanleiding zijn om de netwerkcapaciteit uit te breiden, of te bezien of de beprijzing van datadiensten moet worden aangepast.

In reactie op de beoordeling van het CBP dat de melding van Tele2 bij het CBP onvolledig is, en dat Tele2 in strijd handelt met de informatieplicht uit de artikelen 33 en 34 Wbp, heeft Tele2 [VERTROUWELIJK] conceptteksten toegestuurd; een aanvulling op de melding (Bijlage 2 bij zienswijze 2) en op de voorwaarden (Bijlage 3 bij zienswijze 2).

Ten aanzien van de beoordeling dat Tele2 door doorgifte van persoonsgegevens via [VERTROUWELIJK: A] in strijd handelt met artikel 76 Wbp, handhaaft Tele2 haar standpunt dat geen sprake is van persoonsgegevens, maar biedt Tele2 niettemin aan, indien nodig, een Europese modelbepaling aan te gaan voor doorgifte.

Ten slotte heeft Tele2 nadere inlichtingen verschaft over alternatieven voor haar huidige werkwijze, inclusief een kostenbegroting.¹³

In **bijlage IV** bij dit rapport is de zakelijke inhoud van deze tweede zienswijze van Tele2 opgenomen per onderdeel (met de toevoeging ‘**Zienswijze 2 Tele2**’), 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.

2. FEITELIJKE BEVINDINGEN

2.1 Organisatiebeschrijving

Tele2, gevestigd te Amsterdam en kantoorhoudende te Diemen, is opgericht op 29 mei 1998 en ingeschreven bij de Kamer van Koophandel onder nummer 33303418. De bedrijfsomschrijving van Tele2 is: *“Draadgebonden telecommunicatie. Holding en management, tevens het verlenen van telecommunicatiediensten.”* Tele2 maakt onderdeel uit van de Zweedse Tele2 Group. Tele2 Sverige AB (hierna: Tele2 Zweden) is de moedermaatschappij van Tele2.

Tele2 is geregistreerd bij de ACM als aanbieder van een openbare elektronische communicatiedienst en -netwerk.¹⁴

¹³ Reactie Tele2 op vordering inlichtingen CBP van 21 februari 2013.

¹⁴ Registratie Tele2 URL:

<https://www.acm.nl/nl/onderwerpen/telecommunicatie/registraties/geregistreerde-ondernemingen/resultaat/?query=tele2&x=0&y=0> (URL laatst bezocht op 29 mei 2013).

Tele2 beschrijft zichzelf als “Met meer dan 15 miljoen klanten in 10 landen is Tele2 uitgegroeid tot een toonaangevende Europese telecomspeler.”¹⁵ Tele2 heeft 535.000 abonnees als aanbieder van mobiele telefonie in Nederland.¹⁶ Omgerekend levert dat een marktaandeel op de markt voor abonnees met een (prepaid of postpaid) data abonnement in Nederland op van bijna 2,5%.¹⁷

Tele2 heeft de verwerking van persoonsgegevens, voor zover voor dit onderzoek van belang, op 8 april 2008 (gewijzigd) gemeld bij het CBP onder nummers m1249952 en m1252089 (versienummers 6.0 en 5.0). In de meldingen zijn, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

‘Call Detail Records (verkeersgegevens elektronische communicatie) Tele2 Ned. BV’ (m1249952)

Ten behoeve van de levering van elektronische communicatiediensten en de facturering daarvan.
Beheer van verbruik en verkeer van de elektronische communicatiediensten.
Ten behoeve van marketing- en verkoopactiviteiten.
Nakoming van wettelijke verplichtingen. ¹⁸

‘Tele2 Nederland B.V. algemeen, Verbruiksgegevens/CDR/EDR’ (m1252089)

Het aanbieden en uitvoeren van elektronische communicatiediensten.
Financiële administratie en het factureringsproces. Daaronder begrepen: incasso, klachtbehandeling en het verstrekken van gegevens aan derden t.b.v. het innen van vorderingen.
Het ontwikkelen, uitbreiden en verbeteren van de dienstverlening en producten van Tele2, mede door het informeren van klanten, en m.b.v. (direct) marketing activiteiten en marktonderzoek.
Netwerkbeheer. ¹⁹

¹⁵ URL: <http://newsroom.tele2.nl/over-ons/> (URL laatst bezocht op 29 mei 2013).

¹⁶ Cijfers eind eerste kwartaal 2013. Bron: financiële kwartaalreportage Tele2, URL: <http://reports.tele2.com/2013/Q1/index.html> (URL laatst bezocht op 29 mei 2013). Eind derde kwartaal van 2011 had Tele2 325.000 abonnees. ‘Cijfers mobiel en vaste telefonie Tele2 Nederland dalen’, *Telecompaper* 20 oktober 2011. URL: <http://www.telecompaper.com/nieuws/cijfers-mobiel-en-vaste-telefonie-tele2-nederland-dalen> (URL laatst bezocht op 29 mei 2013).

¹⁷ Omgerekend vanuit het gegeven dat gemiddeld 46,4% van de mobiele abonnees in Nederland ook een data-abonnement heeft, bedient Tele2 bijna 250.000 mobiele abonnees met data-toegang. Dit resulteert in een marktaandeel van 2,4 procent. Bron: financiële kwartaalreportage Tele2 Q1 2013, URL: <http://reports.tele2.com/2013/Q1/index.html> (URL laatst bezocht op 29 mei 2013).

¹⁸ In de melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens onder andere genoemd: ‘Klanten van Tele2’ respectievelijk ‘Verkeersgegevens met betrekking tot elektronische communicatiediensten’.

¹⁹ In de melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) van betrokkenen en gegevens onder andere genoemd: ‘NAW-gegevens’, ‘Telefoon,- faxnummer en emailadres’, ‘IP adres (Radius gegevens) /telefoonnummers’, ‘Verbruiksgegevens/CDR/EDR afgeleid van Radius gegevens, DSLAM-logs of telefoongespreksgegevens’.

Tele2 heeft verklaard dat de meldingen met nummers m1249952 en m1252089 geen betrekking hebben op de verwerking van persoonsgegevens verkregen met behulp van data-analyse technieken in haar mobiele netwerk: *“De door [VERTROUWELIJK: apparatuur] gegenereerde gegevens zijn niet tot klanten te herleiden en zijn daarom geen persoonsgegevens. De in de vraag [van het CBP, toevoeging door het CBP] genoemde meldingen zien daarom niet deze gegevens uit [VERTROUWELIJK: apparatuur] . Wel is het zo dat Tele2 [VERTROUWELIJK] de door [VERTROUWELIJK: apparatuur] gegenereerde statistische data mede gebruikt voor marketing doeleinden in algemene zin. In zoverre is dus net als bij de genoemde meldingen sprake van gebruik van data ter ondersteuning van marketing- en verkoopactiviteiten, en voor netwerkbeheer en de ontwikkeling van klantenprofielen. Het gaat daarbij echter niet om aan individuele klanten gerelateerde profielen of aanbiedingen, maar om het verbeteren van haar algemene dienstenaanbod.”*²⁰

Tele2 heeft geen andere meldingen gedaan die betrekking hebben op de verwerking van gegevens over en uit het dataverkeer bij de inzet van data-analyse technieken in haar mobiele netwerk ten behoeve van de hierboven genoemde doeleinden. Tele2 heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp. Tele2 heeft begin 2012 een compliance-officer aangesteld, die zich mede richt op de naleving van de privacy-regelgeving.²¹

Voorgestelde maatregel

Tele2 heeft bij haar tweede zienswijze een concept gewijzigde melding gevoegd.²²

Hierin meldt Tele2 als doeleinden enerzijds het analyseren en de opslag van geanonimiseerde gegevens ten behoeve van netwerkbeheer en anderzijds het verwerken van mobiel dataverkeer om het in geanonimiseerde vorm te analyseren en op te slaan.

In de concept gewijzigde melding worden de volgende soorten gegevens genoemd: [VERTROUWELIJK].²³

2.2 Mobiel netwerk, netwerkverkeer en plaatsing data-analyse apparatuur

Tele2 is een zogeheten ‘full’ Mobile Virtual Network Operator (MVNO).²⁴ Tele2 heeft geen GSM- of UMTS-vergunning/radiotoegangsnetwerk (waaronder zendmasten), maar koopt sinds medio 2009²⁵ radiotoegang in tot het mobiele netwerk van T-Mobile.

²⁰ Reactie Tele2 op verzoek om inlichtingen van 8 september 2011, p. 4.

²¹ Zienswijze 1 Tele2, randnummer 19, zie **bijlage III** bij dit rapport.

²² Zienswijze 2 Tele2, bijlage 2, zie **bijlage IV** bij dit rapport.

²³ Idem.

²⁴ Een ‘full’ MVNO is een mobiele aanbieder die alleen gebruik maakt van de basis (zendmast) infrastructuur van een *Mobile Network Operator* (MNO), maar alle spraak en datadiensten zelf levert. Vgl het statement van de directeur van Tele2 NL, “Tele2 NL bezit een uitgebreid glasnetwerk dat gebruikt kan worden als backhaul voor de grote databehoeft van 4G en de nodige apparatuur vanwege het feit dat het reeds een ‘full MVNO’ is”, 8 september 2011, <http://newsroom.tele2.nl/2011/09/gunther-vogelpoel-over-toekomst-mobiele-markt-in-telecompaper/> (URL laatst bezocht op 29 mei 2013).

²⁵ ‘T-Mobile en Tele2 sluiten MVNO partnership voor mobiele diensten’, Persbericht Tele2 19 februari 2009. URL: <http://newsroom.tele2.nl/wp->

[VERTROUWELIJK].²⁶

Tele2 maakt gebruik van data-analyse technieken op het dataverkeer in haar mobiele netwerk.²⁷ [VERTROUWELIJK]. Daarnaast gebruikt Tele2 data-analysetechnieken op het e-mailverkeer in haar mobiele netwerk via haar bestaande mailplatform voor vaste (breedband) internettoegang.

Met gebruikmaking van de data-analyse apparatuur inspecteert en analyseert Tele2 *headers* [VERTROUWELIJK]. Daartoe worden datapakketten door/langs een filter met inspectieregels geleid.

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 payload (de 'brief').

Tele2 verkrijgt via de data-analyse apparatuur gegevens over het dataverkeer van alle²⁸ naar schatting 250.000 Tele2 abonnees met een (prepaid of postpaid) data-abonnement²⁹ en van de gebruikers van haar dataverkeersdiensten.

Van het totaal aantal Tele2 mobiele telefonie abonnees met mobiel internet hebben er volgens Tele2 ongeveer [VERTROUWELIJK] een prepaid aansluiting. [VERTROUWELIJK]. Tele2 verklaart dat zij schat identificerende gegevens te hebben van [VERTROUWELIJK] van de prepaid abonnees.³⁰

[VERTROUWELIJK]

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.

De headergegevens in lagen 2 tot en met 7 zijn in dit rapport gedefinieerd als gegevens 'over' het dataverkeer.

content/uploads/2011/01/090219_Persbericht_T-Mobile-en-Tele2-sluiten-MVNO-partnership.pdf (URL laatst bezocht op 29 mei 2013).

²⁶ Persbericht Tele2 19 februari 2009: "*Dat betekent dat Tele2 zelfstandig spraak-, SMS- en mobiele breedband diensten ontwikkelt en aanbiedt aan zijn klanten in Nederland.*"

²⁷ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 1-2. E-mail Tele2 aan OPTA van 25 mei 2011 en reactie Tele2 op verzoek om inlichtingen OPTA van 30 mei 2011.

²⁸ Idem, p. 2. [VERTROUWELIJK]

²⁹ Aan het einde van het eerste kwartaal van 2013 had Tele2 535.000 mobiele telefonieabonnees in Nederland. De schatting van 250.000 mobiele aansluitingen met data-abonnement berust op het gemiddelde percentage uit de ACM Openbare rapportage mobiel Q4 2012 van 46,4 procent van mobiele telefonie-aansluitingen met data-abonnement. Zie voetnoot 6.

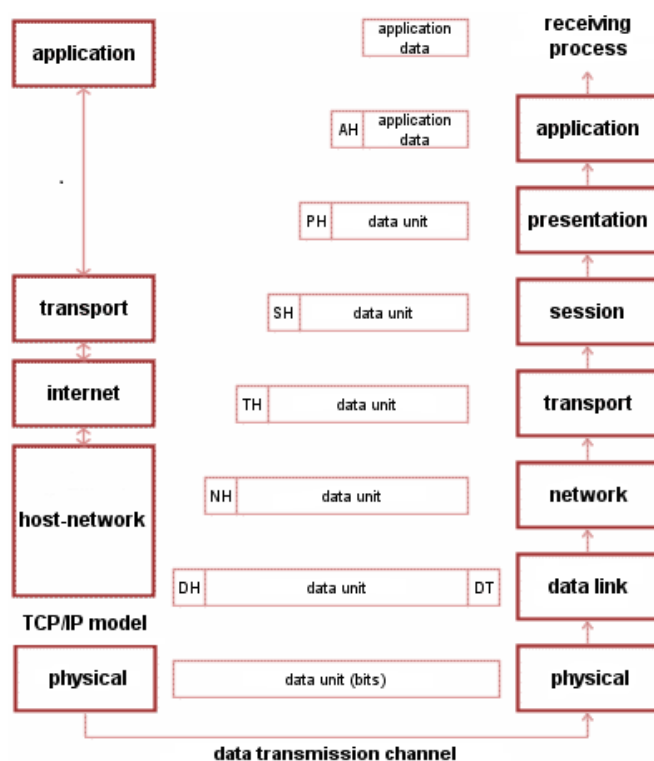
³⁰ Reactie Tele2 op verzoek om inlichtingen van 11 april 2012, p. 2.

Het bestemmings- en afzender-IP-adres zitten in laag 3/4. Dit kan technisch worden gezien als de adressering op de buitenste envelop: gegevens die noodzakelijk zijn om het verkeer op de bestemming af te leveren.

Vanaf laag 4 (transportlaag) bevatten de headers gedetailleerde informatie over gebruikte apps en bezochte websites, zoals het gebruikte protocol, de frequentie (het aantal keren dat verbinding wordt gemaakt) en de *hostname* (URL op hoofddomein). Inhoud van het verkeer/payload is in dit rapport gedefinieerd als gegevens 'uit' het dataverkeer.

[VERTROUWELIJK].

AFBEELDING I opbouw packets volgens TCP-IP en OSI-model³¹



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.

³¹ Bron: URL: http://www2.themanualpage.org/networks/networks_osi2.php3 (URL laatst bezocht op 29 mei 2013).

2.3 Doeleinden

Tele2 heeft verklaard dat er (limitatief) twee doeleinden zijn (waren) voor de toepassing van data-analyse technieken in haar mobiele netwerk. De twee doeleinden zijn:

- | |
|--|
| 1. Het genereren van verkeersstatistieken van het mobiele internetverkeer voor netwerkbeheer ³² en marketingdoeleinden (hierna: marktonderzoeksdoeleinden). ³³ Voor ‘ <i>traffic management</i> ’, bijvoorbeeld om capaciteitsbeperkingen en <i>heavy use</i> in het netwerk te identificeren (en congestie tegen te gaan), om de dienstverlening te optimaliseren voor zowel <i>realtime</i> als non <i>realtime</i> verkeer, en om de prijs/kwaliteitverhouding voor klanten voortdurend te optimaliseren. ³⁴ |
| 2. Afhandelen van verkeer van prepaid klanten naar opwaardeersites. ³⁵ |

In haar ‘Fair Use Policy voor mobiele openbare elektronische communicatiediensten van Tele2’ schrijft Tele2 over haar beleid met betrekking tot e-mails dat zij e-mails aan de afzender onder andere zal blokkeren en deze zonder kennisgeving zal verwijderen als een attachment virus, spyware of andere schadelijke gegevens bevat, en als een attachment een bepaalde (niet toegestane) extensie heeft, zoals '.pif', '.scr', '.cmd', '.bat' of '.com'.³⁶ Tele2 heeft desgevraagd, in reactie op een mondeling verzoek om inlichtingen, over de inzet van data-analyse technieken op de inhoud van e-mails (inclusief attachments) voor spam- en virusfiltering verklaard dat zij het inkomende en uitgaande mobiele e-mailverkeer van haar abonnees door een e-mailplatform leidt dat (ook) in gebruik is voor abonnees met een (vast) breedband ADSL-abonnement en dat daarop data-analyse technieken worden toegepast.³⁷ Deze inzet van data-analyse technieken wordt als derde doeleinde in dit rapport besproken.

Hierna worden de gegevensverwerkingen voor de hierboven genoemde drie doeleinden besproken.

In haar correspondentie met OPTA heeft Tele2 nog een ander doeleinde genoemd voor de inzet van data-analyse technieken in haar mobiele netwerk, namelijk het herkennen van MMS-verkeer om dubbele facturering van MMS te voorkomen.³⁸ Tele2 verklaart hierover: “*Inmiddels heeft Tele2 per 8 juni 2011, op basis van afnemende vraag, de*

³² Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2. Reactie Tele2 op verzoek om inlichtingen OPTA van 30 mei 2011, p. 2: [VERTROUWELIJK].

³³ Idem, p. 4: “*Wel is het zo dat Tele2 [VERTROUWELIJK] de door [VERTROUWELIJK: apparatuur] gegenereerde statistische data mede gebruikt voor marketing doeleinden in algemene zin.*”

³⁴ Idem, p. 2.

³⁵ Idem. Zie ook e-mail Tele2 aan OPTA van 25 mei 2011.

³⁶ Fair Use Policy voor mobiele openbare elektronische communicatiediensten van Tele2 (geldig vanaf 1 mei 2011), URL: http://www.tele2.nl/files/Fair_Use_Policy_Mobiele_telefoondiensten-2011.pdf (URL laatst bezocht op 29 mei 2013).

³⁷ Mondelinge inlichtingen Tele2 van 3 augustus 2012.

³⁸ E-mail Tele2 aan OPTA van 25 mei 2011 en reactie Tele2 op verzoek om inlichtingen OPTA van 30 mei 2011, p. 1. Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2.

MMS user case ten behoeve van het limiteren van datakosten ten behoeve van gebruikers, beëindigd. De MMS user case was ingevoerd in 2007.”³⁹

Vanwege de beëindiging van de inzet van data-analyse technieken in haar mobiele netwerk voor (de facturering van) MMS-verkeer is de gegevensverwerking voor dat doeleinde niet door het CBP beoordeeld.

2.4 Netwerkbeheer en marktonderzoeksdoeleinden

Als eerste verzamel- en verwerkingsdoeleinde van gegevens noemt Tele2 netwerkbeheer en marktonderzoeksdoeleinden (daaronder mede begrepen het identificeren van capaciteitsproblemen en het voorkomen van congestie).⁴⁰

Aanleiding inzet data-analyse technieken

Tele2 verklaart vanaf het derde kwartaal van 2010 *Deep Packet Inspection* (DPI) toe te passen op gegevens met betrekking tot het mobiele dataverkeer. Tele2 schrijft in dat verband: *“De laatste user case betrof het vastleggen van Tele2 [VERTROUWELIJK] verkeersstatistieken sinds Q3 2010 tot heden. Zoals hierna wordt toegelicht, wordt hierbij Deep Packet Inspection toegepast.”⁴¹*

Over het gebruiksdoel van deze verkeersstatistieken verklaart Tele2:

“De verkeersstatistieken worden gebruikt in het kader van ‘traffic management’, bijv. om capaciteitsbeperkingen en heavy use in het netwerk te identificeren (en congestie tegen te gaan), om de dienstverlening te optimaliseren voor zowel realtime verkeer als non realtime verkeer, en om de prijs/kwaliteit verhouding voor onze klanten voortdurend te optimaliseren.”⁴²

Aanvullend heeft Tele2 toegelicht dat de verkeersstatistieken niet alleen worden gebruikt om de benodigde netwerkcapaciteit in de nabije toekomst te voorspellen, maar ook voor het overwegen van alternatieven zoals [VERTROUWELIJK].⁴³

Tele2 illustreert met een aantal voorbeelden dat fluctuaties in het dataverkeer moeilijk voorspelbaar zijn. *“Aanbieders van mobiel internet bevinden zich in terra incognita. (...) De lancering van een nieuw toesteltype of het onverwachte succes van een bepaalde app kan plotseling leiden tot een enorme toename van het dataverkeer.”⁴⁴* Tele2 noemt daarbij gebruikers die kennelijk voorop lopen in het gebruik van nieuwe apps en/of nieuwe toestellen. Hun gedrag kan daardoor een aanwijzing vormen voor een significante toename van het dataverkeer.⁴⁵

Tele2 licht in haar zienswijze 1 toe dat de netwerkbelasting die smartphones en apps veroorzaken niet op andere manieren kan worden gemeten, zoals met algemene

³⁹ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2.

⁴⁰ Idem, p. 2 en 4. Reactie Tele2 op verzoek om inlichtingen OPTA van 30 mei 2011, p. 2.

⁴¹ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2.

⁴² Idem.

⁴³ Reactie Tele2 op vordering inlichtingen CBP van 21 februari 2013, p. 2.

⁴⁴ Zienswijze 2 Tele2, randnummer 11. Zie **bijlage IV** bij dit rapport.

⁴⁵ Idem, randnummers 15-16.

marktmonitors en klantenpanels, omdat Tele2 daaraan geen nauwkeurige informatie kan ontlelen welk gebruik klanten daadwerkelijk maken van het mobiele netwerk.⁴⁶

Gevraagd door het CBP naar de mogelijkheid van een steekproefsgewijze toetsing van netwerkgebruik, middels een selecte of aselecte steekproef, heeft Tele2 een docent geconsulteerd [VERTROUWELIJK] gespecialiseerd in *social statistics*, [VERTROUWELIJK]. [VERTROUWELIJK] visie luidt (samengevat) als volgt.

Het volgen van een kleine groep klanten (die daartoe toestemming hebben gegeven, een selecte steekproef) leidt waarschijnlijk tot vertekening en wordt daarom door [VERTROUWELIJK] verder niet besproken.

Omdat er sprake is van scheve verdelingspatronen (een relatief klein deel van de klanten verbruikt een groot deel van het datavolume), dient de aselecte steekproef 50% of meer van de klanten te beslaan. Omdat in dit geval klanten door de tijd heen moeten worden gevolgd (longitudinale data), schrijft [VERTROUWELIJK], is de duur en de representativiteit van de steekproef van groot belang. Om het gedrag per klant (datagebruik en type toestel) goed in beeld te krijgen zouden eerst alle klanten een tijd moeten worden gevolgd. In verband met de voortdurende verandering van het klantgedrag, moet de steekproef bovendien minimaal elke zes maanden opnieuw worden genomen.⁴⁷

Het CBP stelt vast dat het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, (de gevolgen van) de toename van het datavolume relativeert in de recente 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, 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.”*⁴⁸

Data-analyse apparatuur

Tele2 gebruikt data-analyse apparatuur van de [VERTROUWELIJK] leverancier [VERTROUWELIJK: A] voor het doeleinde netwerkbeheer en marktonderzoeksdoeleinden.⁴⁹

De [VERTROUWELIJK: apparatuur] wordt door Tele2 gebruikt om verkeersstatistieken te genereren.⁵⁰

⁴⁶ Zienswijze 1 Tele2, randnummer 64. Zie **bijlage III** bij dit rapport.

⁴⁷ Reactie Tele2 op vordering inlichtingen CBP van 21 februari 2013, p. 4-5.

⁴⁸ BEREC Guidelines for quality of service in the scope of net neutrality dated 26 November 2012, p.17. URL:

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

⁴⁹ Het betreft [VERTROUWELIJK]. Reactie Tele2 op rappel verzoek om inlichtingen van 23 november, p. 2-3.

De data-apparatuur bevindt zich fysiek in [VERTROUWELIJK].⁵¹ Tele2 verklaart in dat verband: [VERTROUWELIJK].

[VERTROUWELIJK]

Tele2 licht nader toe: [VERTROUWELIJK].⁵²

Uit de (contracts)documentatie bij de [VERTROUWELIJK: apparatuur] volgt dat de data-analyse apparatuur in staat is om [VERTROUWELIJK]. In april 2012 bevatte [VERTROUWELIJK: apparatuur] meer dan 2.000 signatures van verschillende apps en protocollen⁵³, zoals http, smtp, ftp, [VERTROUWELIJK], verbindingen met de encryptie standaarden SSL en SSH en bijvoorbeeld als het om VoIP (internettelefonie) gaat, [VERTROUWELIJK].⁵⁴

Herkenning/identificatie vindt volgens de leverancier plaats op gedetailleerd niveau: [VERTROUWELIJK].

[VERTROUWELIJK]

Bezoek aan en gebruik van apps, websites en protocollen

De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze met behulp van vooraf gedefinieerde en ingestelde filtermodules gegevens verzamelt⁵⁵, vastlegt⁵⁶ en bewaart⁵⁷ over het bezoek aan en gebruik van apps, websites (op het niveau van hostnames) en protocollen zoals het type verkeer, de duur en het verbruikte datavolume per service⁵⁸ en per type smartphone.⁵⁹

De [VERTROUWELIJK: apparatuur] herkent/identificeert meer dan [VERTROUWELIJK] vooraf gedefinieerde apps, websites (op hostname niveau) en protocollen, zoals http, smtp, ftp, [VERTROUWELIJK], verbindingen met de encryptie standaarden SSL en SSH⁶⁰ en bijvoorbeeld als het om VoIP (internettelefonie) gaat, [VERTROUWELIJK].⁶¹

⁵⁰ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2.

⁵¹ Idem.

⁵² Reactie Tele2 op rappel verzoek om inlichtingen van 2 december 2011, p. 2.

⁵³ URL: [VERTROUWELIJK]

⁵⁴ Bijlage screenshot Traffic (MiB) voor genoemde apps/protocollen bij reactie Tele2 op vordering inlichtingen CBP van 13 december 2011.

⁵⁵ [VERTROUWELIJK].

⁵⁶ [VERTROUWELIJK].

⁵⁷ [VERTROUWELIJK].

⁵⁸ Bijlage screenshot Traffic (MiB) voor genoemde apps/protocollen bij reactie Tele2 op informatievordering van 13 december 2011.

⁵⁹ Bijlage 4 bij reactie Tele2 op verzoek om inlichtingen van 19 september, figuur 5: top 10 van [VERTROUWELIJK] naar hoeveelheid verkeer van en naar [VERTROUWELIJK].

⁶⁰ [VERTROUWELIJK].

⁶¹ Bijlage screenshot Traffic (MiB) voor genoemde apps/protocollen bij reactie Tele2 op informatievordering van 13 december 2011.

Aanvankelijk verklaarde Tele2: *"Tele2 monitort niet op specifieke applicaties."*⁶² Uit de screenshots die Tele2 aan het CBP heeft verstrekt, gecontroleerd aan de hand van de (contracts)documentatie bij de [VERTROUWELIJK: apparatuur], blijkt echter dat de data-analyse apparatuur bijvoorbeeld statistieken genereert van de websites die het meeste verkeer genereren.⁶³

In reactie op een verzoek om aanvullende inlichtingen voegt Tele2 daaraan toe dat Tele2 een beperkt aantal onderdelen van de dienstverlening opslaat voor statistische doeleinden, [VERTROUWELIJK].⁶⁴ Tele2 verklaart verder dat de verkeersstatistieken ook betrekking hebben op land, [VERTROUWELIJK], type verkeer en verkeer per netwerkgebruiker.⁶⁵

Tele2 verklaart geen individuele klantgegevens nodig te hebben over bezoek aan websites en gebruik van apps en protocollen voor het vaststellen van trendstatistieken voor verkeersbeheer: [VERTROUWELIJK].⁶⁶

In haar zienswijze 1 geeft Tele2 aan dat de [VERTROUWELIJK: apparatuur]-technologie alleen screent op een beperkt aantal vooraf gedefinieerde signatures. Dit betreft hostnames, en geen volledige URL's. De techniek is voor Nederlandse klanten op zeer beperkte schaal ingezet. [VERTROUWELIJK].⁶⁷

Tele2 licht in haar zienswijze 2 toe de volgende soorten gegevens nodig te hebben per individuele klant: [VERTROUWELIJK].⁶⁸

Technisch vindt de gegevensverwerking door Tele2 als volgt plaats.

Data- en signaleringsverkeer packets van alle Tele2 abonnees worden realtime door/langs een filter met inspectieregels geleid. De gedetecteerde gegevens met betrekking tot het bezoek aan en gebruik van de vooraf gedefinieerde websites, apps en protocollen worden vervolgens per abonnee geordend.⁶⁹

Tele2 verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement, bijvoorbeeld enerzijds [VERTROUWELIJK: identifiers], en anderzijds de hostname (URL op hoofddomein), het IP-adres van naar⁷⁰, de gebruikte

⁶² E-mail Tele2 aan OPTA van 25 mei 2011.

⁶³ Bijlage voorbeelden [VERTROUWELIJK] user interface bij brief van Tele2 van 19 september 2011, figuur 1, onderdeel [VERTROUWELIJK]

⁶⁴ Reactie Tele2 op verzoek om inlichtingen van 2 november 2011, p. 1.

⁶⁵ Reactie Tele2 op verzoek om inlichtingen van 19 september, p. 3. Tele2 noemt hier, kennelijk abusievelijk, ook de URL als gegeven waar de verkeersstatistieken betrekking op hebben, maar ontkent dit nadrukkelijk bij brief van 2 november 2011 en in zienswijze 1.

⁶⁶ Reactie Tele2 op verzoek om inlichtingen van 9 november 2011, p. 3

⁶⁷ Zienswijze 1 Tele2, randnummers 31 en 32. Zie **bijlage III** bij dit rapport

⁶⁸ Reactie Tele2 van 21 februari 2013 op vordering inlichtingen CBP, p. 2-3. Zie ook **bijlage IV** bij dit rapport

⁶⁹ [VERTROUWELIJK].

⁷⁰ [VERTROUWELIJK]. Reactie Tele2 op rappel verzoek om inlichtingen van 2 december 2011, p. 1.

service/protocol, [VERTROUWELIJK] evenals aantallen bytes (volume)⁷¹, duur en frequentie.

Vervolgens wordt een deel van deze gegevens per abonnee in de achterliggende database(s)/bestanden opgeslagen⁷² en gedurende maximaal twaalf maanden bewaard.⁷³

De [VERTROUWELIJK: apparatuur] legt voor de duur van de datasessie van een abonnee naast het [VERTROUWELIJK: identifier] ook [VERTROUWELIJK: identifiers] vast, in niet-permanent (werk) geheugen.

Daarna wordt [VERTROUWELIJK: identifier] in gehashte vorm opgeslagen.⁷⁴ [VERTROUWELIJK: identifier] wordt alleen opgeslagen als [VERTROUWELIJK] (zonder verdere details).⁷⁵ De [VERTROUWELIJK: identifiers] en de locatiegegevens worden niet opgeslagen.⁷⁶

Via een gebruikersinterface kunnen onder andere de volgende gegevens worden geraadpleegd: top web hosts en apps/protocollen, top subscribers naar dataverbruik (heavy user abonnee) en top [VERTROUWELIJK], in combinatie met het versleutelde [VERTROUWELIJK: identifier].⁷⁷

Versleuteling door [VERTROUWELIJK: B]

De versleuteling van [VERTROUWELIJK: identifier], als hierboven genoemd, vindt plaats in [VERTROUWELIJK].

Tele2 [VERTROUWELIJK] heeft een overeenkomst gesloten met [VERTROUWELIJK: B] met betrekking tot de versleuteling van [VERTROUWELIJK: identifier]. [VERTROUWELIJK: B] is sinds augustus 2006 een 100% dochteronderneming van [VERTROUWELIJK: A], [VERTROUWELIJK]. Uit de overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: B] blijkt dat [VERTROUWELIJK: B] een encryptiesleutel op de [VERTROUWELIJK: apparatuur] levert [VERTROUWELIJK]. De aansprakelijkheid van partijen in geval van wanprestatie is daarbij beperkt tot in totaal ten hoogste ongeveer [VERTROUWELIJK].⁷⁸

⁷¹ Reactie Tele2 op verzoek om inlichtingen van 19 september, p.3 [VERTROUWELIJK]. Vgl ook de bijlage met Screenshot [VERTROUWELIJK: apparatuur] bij deze reactie van Tele2, [VERTROUWELIJK].

⁷² [VERTROUWELIJK].

⁷³ [VERTROUWELIJK].

⁷⁴ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 3.

[VERTROUWELIJK] Reactie Tele2 op rappel vordering van 20 december 2011, p.1. Bijlage 1 bij reactie Tele2 op rappelvordering van 20 december 2011 [VERTROUWELIJK] Deze verklaring is ondertekend door [VERTROUWELIJK].

⁷⁵ Zienswijze 1 Tele2, randnummer 36. Zie **bijlage III** bij dit rapport.

⁷⁶ Reactie Tele2 op rappel verzoek om inlichtingen van 2 december 2011, p. 1. [VERTROUWELIJK]

⁷⁷ Bijlage screenshot Traffic (MiB) voor genoemde apps/protocollen bij reactie Tele2 op informatievordering van 13 december 2011. Bijlage 4 bij reactie Tele2 op verzoek om inlichtingen van 19 september, figuur 5: [VERTROUWELIJK].

⁷⁸ Overeenkomst inzake [VERTROUWELIJK].

Tele2 licht toe dat [VERTROUWELIJK: B] [VERTROUWELIJK].

Tele2 verklaart in reactie op een verzoek om inlichtingen van OPTA over de getroffen technische en organisatorische maatregelen: [VERTROUWELIJK].

De overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: B] bevat geen technische specificatie(s) over de wijze waarop wordt versleuteld, of welke gegevens worden versleuteld. Uit nadere informatie van Tele2 blijkt dat de hash wordt gemaakt met [VERTROUWELIJK].⁷⁹

Naar aanleiding van het rapport voorlopige bevindingen heeft Tele2 nader onderzoek gedaan naar de gebruikte versleuteling. Tele2 verklaart: [VERTROUWELIJK]

Voorgestelde maatregelen

Op verzoek van het CBP heeft Tele2 een offerte aangevraagd bij haar leverancier [VERTROUWELIJK: A] voor [VERTROUWELIJK]. Alternatief stelt Tele2 voor om [VERTROUWELIJK]. Dit zou volgens de leverancier vergelijkbare kosten met zich meebrengen.⁸⁰

Ondersteuning en onderhoud door [VERTROUWELIJK: A]

Er wordt onderhoud en technische ondersteuning voor de [VERTROUWELIJK: apparatuur] geleverd door [VERTROUWELIJK: A].⁸¹ Tele2 licht in haar zienswijze 1 toe dat dat betekent dat [VERTROUWELIJK: A/B] op afstand actie kan ondernemen om het probleem te verhelpen.⁸²[VERTROUWELIJK].

Tele2 verklaart dat in geval van onderhoud en/of storing [VERTROUWELIJK] toegang kunnen hebben tot het systeem.⁸³ Tele2 licht nader toe: [VERTROUWELIJK].

Tele2 verklaart over de mogelijkheid om in dat kader toegang te krijgen tot de gegevens en encryptiesleutel [VERTROUWELIJK]:⁸⁴

Het CBP leidt hieruit af dat Tele2 hiermee wil zeggen dat [VERTROUWELIJK: B] de encryptiesleutel en/of andere gegevens niet met [VERTROUWELIJK: A] deelt.⁸⁵

In haar zienswijze 1 verklaart Tele2 dat [VERTROUWELIJK].⁸⁶

⁷⁹ Reactie Tele2 op rappel verzoek om inlichtingen van 23 november 2011, p. 2.

⁸⁰ Reactie Tele2 op vordering inlichtingen CBP van 21 februari 2013, p. 7-8.

⁸¹ Overeenkomst [VERTROUWELIJK].

⁸² Zienswijze 1 Tele2, randnummer 67, **Bijlage II** bij dit rapport

⁸³ Reactie Tele2 op rappel verzoek om inlichtingen van 23 november 2011, p. 2. [VERTROUWELIJK].

⁸⁴ Reactie Tele2 op verzoek om inlichtingen van 9 november 2011, p. 2.

⁸⁵ Idem: "Het is dus niet zo dat Tele2 gegevens (laat staan persoonsgegevens) feitelijk aan [VERTROUWELIJK: B] beschikbaar stelt voor verwerking (en dat zij die vervolgens zou kunnen doorspelen naar derden zoals [VERTROUWELIJK: A]). Als dat al anders zou zijn, geldt bovendien dat [VERTROUWELIJK: B] in [VERTROUWELIJK] gevestigd en aan de [VERTROUWELIJK] privacy wetgeving moet voldoen. Aangenomen mag worden dat deze wet adequate waarborgen biedt tegen het eventuele doorspelen door [B] van persoonsgegevens aan derden zoals [VERTROUWELIJK: A]."

⁸⁶ Zienswijze 1 Tele2, randnummer 46. Zie **bijlage III** bij dit rapport.

[VERTROUWELIJK]. Tele2 heeft geen vergunning⁸⁷ verkregen voor doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Tele2 heeft geen (doorgifte)overeenkomst gesloten met [VERTROUWELIJK: A].

Tele2 heeft geen (bewerkers)overeenkomst gesloten met [VERTROUWELIJK: B] of [VERTROUWELIJK: A]. Tele2 verklaart desgevraagd: *“Tele2 heeft inmiddels kunnen vaststellen dat er geen specifieke bewerkersovereenkomst is gesloten tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: B]. (...)”*⁸⁸ Tele2 licht toe: *“Daar bestaat ook geen noodzaak toe, nu [VERTROUWELIJK: B] volgens Tele2 [VERTROUWELIJK] niet kan worden aangemerkt als bewerker als bedoeld in de Wbp, dat wil zeggen: als partij die ten behoeve van Tele2 [VERTROUWELIJK] persoonsgegevens verwerkt. Zoals uit de eerder gegeven antwoorden blijkt, is de rol van [VERTROUWELIJK: B] die van een leverancier van een product (een appliance bestaande uit hardware en software). [VERTROUWELIJK].*

Voorgestelde maatregelen

Tele2 geeft in haar zienswijze 1 aan bereid te zijn om met [VERTROUWELIJK: A/B] in overleg te treden over het aangaan van een bewerkers- en doorgifteovereenkomst.

Bij haar zienswijze 2 heeft Tele2 een conceptovereenkomst bijgevoegd tussen Tele2 [VERTROUWELIJK]⁸⁹

De concept bewerkersovereenkomst bevat een verplichting voor [VERTROUWELIJK: B] om de persoonsgegevens slechts in opdracht van Tele2 te verwerken: [VERTROUWELIJK].

De concept bewerkersovereenkomst bevat verder een verplichting voor [VERTROUWELIJK: B] om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, volgens het recht van [VERTROUWELIJK].

De concept bewerkersovereenkomst bevat ten slotte een bepaling dat [VERTROUWELIJK: B] gehoor zal geven aan een redelijk verzoek van Tele2 om te verifiëren of zij handelt in overeenstemming met haar verplichtingen als bewerker: [VERTROUWELIJK].

De concept bewerkersovereenkomst bevat ten aanzien van [VERTROUWELIJK: A] onder andere de bepaling dat Tele2 en [VERTROUWELIJK: A] zich zullen houden aan de overgelegde concept doorgifte-overeenkomst tussen Tele2 (data exporter) en [VERTROUWELIJK: A] (data importer) (toegevoegd Annex 1 bij de concept bewerkersovereenkomst). De concept doorgifte-overeenkomst bevat verplichtingen voor [VERTROUWELIJK: A] om de persoonsgegevens slechts in opdracht van Tele2 te verwerken en passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige

⁸⁷ Als bedoeld in artikel 77, tweede lid, van de Wbp.

⁸⁸ Reactie Tele2 op rappel verzoek om inlichtingen van 30 november 2011, p. 1. [VERTROUWELIJK]

⁸⁹ Zienswijze 2 Tele2, randnummer 64. Zie **bijlage IV** bij dit rapport.

verwerking (volgens het recht van [VERTROUWELIJK]), afspraken over toezicht op de naleving van de afspraken in de bewerkersovereenkomst, de categorieën van verwerkte persoonsgegevens, de doeleinden (activities relevant to the transfer en processing operations) en afspraken over het al dan niet toestaan van verwerking door subbewerkers.

Tele2 heeft bij deze tweede zienswijze tevens een concept doorgifte-overeenkomst gevoegd tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A], op basis van de model doorgiftebepalingen van de Europese Commissie, waarbij Tele2 [VERTROUWELIJK] als verantwoordelijke optreedt, en [VERTROUWELIJK: A] als bewerker.⁹⁰

Bij haar zienswijze 2 heeft Tele2 tevens een concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A] gevoegd. Tele2 gebruikt voor de concept doorgifte-overeenkomst het door de Europese Commissie goedgekeurde modelcontract voor doorgifte naar een bewerker in een derde land (Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)).⁹¹ Tele2 heeft de bepalingen van het modelcontract ongewijzigd overgenomen.

Appendix 2 bij de concept doorgifte-overeenkomst/het modelcontract (Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached)) is thans nog niet ingevuld: [VERTROUWELIJK]

Informatie voor abonnees

De 'Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten' bevatten de volgende informatie over de verwerking van gegevens ten behoeve van netwerkbeheer en marktonderzoeksdoeleinden:

"(...) Tele2 verzamelt en verwerkt (persoons)gegevens van de Klant, in overeenstemming met de geldende privacywetgeving. Onder (persoons)gegevens worden mede Verkeersgegevens begrepen.

(...) Tele2 verzamelt en verwerkt (persoons)gegevens van de Klant voor zover deze nodig zijn voor een goede dienstverlening aan de Klant. Deze gegevens worden door Tele2 verwerkt en zonodig verstrekt aan derden, voor de volgende doeleinden:

a. de goede dienstverlening en de verdere ontwikkeling van de dienstverlening; (...)

e. netwerkbeheer en de bevordering van een efficiënte inrichting van de bedrijfsprocessen;

f. marktonderzoek- en direct marketingdoeleinden;

h. het voldoen aan wettelijk verplichtingen (...).

⁹⁰ Zienswijze 1 Tele2, randnummers 70 en 73 en Zienswijze 2 Tele2, bijlagen 3 en 4 bij deze zienswijze. Zie de **bijlagen III** en **IV** bij dit rapport.

⁹¹ URL: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (URL laatst bezocht op 29 mei 2013).

*(...) Tele2 bewaart de verzamelde persoonsgegevens niet langer dan noodzakelijk is voor de in dit artikel genoemde doeleinden en draagt zorgt voor passende technische en organisatorische maatregelen ter beveiliging van de persoonsgegevens.*⁹²

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

Tele2 had tot april 2013, voor zover voor dit onderzoek van belang⁹³, geen algemene privacy-verklaring.

Voorgestelde maatregel

Tele2 heeft bij haar tweede zienswijze een voorstel gevoegd om de informatie uit te breiden. [VERTROUWELIJK].⁹⁴

Getroffen maatregel

In april 2013 heeft Tele2 een (algemeen) Privacy Statement gepubliceerd op haar website.⁹⁵ Dit Privacy Statement bevat de volgende informatie over de gegevensverwerkingen voor netwerkbeheer en marktonderzoek:

Verkeersgegevens

In het kader van onze dienstverlening verwerken wij verschillende soorten gegevens die nodig zijn om bel- internet en televisieverkeer over ons netwerk te vervoeren, die hierna worden opgesomd. Hierbij worden verkeersgegevens verwerkt die informatie geven over het gebruik en verbruik van onze diensten, maar die niet de inhoud van de communicatie zelf betreffen.

Onder het kopje 'Internetgegevens' schrijft Tele2:

De datum, het tijdstip en de duur van een internet sessie, technische identificatiegegevens (zoals je gebruikersnaam en wachtwoord van Tele2-diensten), e-maildienst, de applicatieserver waarmee apps die jij gebruikt verbinding maken, je IP- adres, de route die jouw dataverkeer heeft afgelegd over ons netwerk, datavolume en de kwaliteit van je verbinding (denk aan foutmeldingen).

Onder het kopje '(Direct) marketing- en verkoopdoeleinden' schrijft Tele2:

Verkeersgegevens gebruiken wij om op geaggregeerd niveau (d.w.z. dat deze gegevens niet worden herleid naar individuele personen) analyses te kunnen maken van het bel-, internet- en kijkgedrag van onze klanten. (...)

Het statement bevat een aparte paragraaf 'Netwerkkwaliteit & Beveiliging'. Onder het kopje 'Inzet van data-analyse techniek' schrijft Tele2: *Voor de planning en het beheer van ons mobiele datanetwerk en de beveiliging daarvan, zet Tele2 data- analyse technieken in. Met*

⁹² Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten (versie geldig vanaf 1 september 2009). URL: http://www.tele2.nl/files/AV_Mobiel_Internet.pdf, tevens aangetroffen op URL: http://www.tele2.nl/files/Algemene_Voorwaarden_-_Mobiel_Internet.pdf (URLs laatst bezocht op 29 mei 2013).

⁹³ Het toepassingsbereik van de algemene Privacy Policy van Tele2 was tot april 2013: *“voor bezoekers van de websites die via <http://www.tele2.nl> toegankelijk zijn.”* URL: <http://www.tele2.nl/algemeen/privacy-policy.html> (URL laatst bezocht op 4 maart 2013).

⁹⁴ Zienswijze 2 Tele2, bijlage 3, zie **bijlage IV** bij dit rapport..

⁹⁵ Privacy Statement Tele2 (april 2013), URL: <http://www.tele2.nl/files/privacy-statement-10-01-2013.pdf> (URL laatst bezocht 29 mei 2013).

behulp daarvan verzamelen en verwerken wij gegevens met betrekking tot het gebruik dat onze klanten maken van mobiele datadiensten. Hiertoe worden gegevens verzameld zoals het toesteltype en de apps die je gebruikt, de bezochte webdomeinen, en het dataverbruik op een bepaald moment. Deze gegevens worden per klant in geanonimiseerde vorm opgeslagen voor analyse ten behoeve van netwerkbeheer. Hierbij wordt niet naar de inhoud van het verkeer gekeken.

Onder het kopje 'Hoe lang worden gegevens bewaard?' schrijft Tele2: *Tele2 streeft ernaar gegevens niet langer te bewaren dan noodzakelijk. Dat betekent bijvoorbeeld dat we gegevens waarmee de factuur is berekend, vernietigen of anonimiseren zodra de factuur is voldaan. Wij moeten ons daarbij voor sommige gegevens wel houden aan de wettelijke bewaartermijn uit de Wet Bewaarplicht. Indien je je abonnement bij Tele2 opzegt, blijven je verkeersgegevens daarom conform de Wet Bewaarplicht in ieder geval nog 6 maanden inzichtelijk voor wat betreft internettoegang en e-mail en tot 12 maanden voor vaste en mobiele telefonie. (...)*⁹⁶

2.5 Prepaidverkeer

Als tweede verwerkingsdoeleinde van gegevens noemt Tele2 om het bezoek van prepaid abonnees aan (gratis) opwaardeersites te faciliteren bij een ontoereikend prepaid tegoed.⁹⁷

Data-analyse apparatuur

Tele2 gebruikt(e) vanaf april 2010 software op de [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] ten behoeve van (de facturering van) prepaidverkeer.⁹⁸

Technisch vond de gegevensverwerking door Tele2 als volgt plaats.

Een prepaid abonnee betaalt vooraf voor het gebruik van datadiensten. Tele2 houdt het tegoed van de prepaid abonnee bij in een factureringssysteem. [VERTROUWELIJK]. Als het tegoed van de abonnee ontoereikend is, geeft het factureringssysteem geen toestemming voor een verbinding en zal de datasessie niet slagen.

[VERTROUWELIJK]

Bij brief van 11 april 2012 heeft Tele2 aangegeven: *"Ten aanzien van de (door [VERTROUWELIJK]) geleverde data-analyse technologie om prepaid klanten in staat te stellen gratis hun tegoed op te waarderen, geldt dat daarvan binnen Tele2 thans geen gebruik wordt gemaakt."*⁹⁹

⁹⁶ Idem.

⁹⁷ E-mail Tele2 aan OPTA van 25 mei 2011: [VERTROUWELIJK] Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2.

⁹⁸ Idem.

⁹⁹ Reactie Tele2 op verzoek om inlichtingen van 11 april 2012, p. 2.

Informatie voor abonnees

Het CBP stelt vast dat er in de 'Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten' geen informatie wordt (werd) gegeven over de verwerking van gegevens ten behoeve van het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed.

Tele2 had tot april 2013 geen algemene privacy-verklaring.¹⁰⁰ In het Privacy Statement van april 2013 is (logischerwijs, omdat de verwerking is gestaakt) geen informatie opgenomen over deze gegevensverwerking.

2.6 Spam-, virus- en spywarefiltering van e-mailverkeer

Als derde verwerkingsdoeleinde van gegevens identificeert het CBP spam-, virus- en virusfiltering van e-mailverkeer.¹⁰¹

Tele2 inspecteert en analyseert het e-mailverkeer¹⁰² van al haar abonnees met een (prepaid of postpaid) data abonnement en zorgt ervoor dat ongevraagde e-mail (met spam, virussen, spyware) tegen wordt gehouden en verwijderd.¹⁰³ Tele2 gebruikt voor dit doeleinde een e-mailplatform dat (ook) in gebruik is voor abonnees met een (vast) breedband ADSL-abonnement.

De data-analyse vindt alleen plaats op e-mail (inclusief attachments) van-en-naar het Tele2-domein (dat wil zeggen: van abonnees met een e-mailadres van Tele2).

Het is (ook) volgens het CBP algemeen aanvaard dat e-mail aanbieders naar de inhoud van e-mails moeten kijken (naar de data inhoud van packets) om spam te kunnen herkennen. Dit gebeurt bij Tele2 vooral aan de hand van de onderwerpsregel van de e-mail.¹⁰⁴ Dat gebeurt bijvoorbeeld aan de hand van veelgebruikte woorden, zoals 'Viagra'. Bij de bestrijding van virussen en spyware worden over het algemeen lijsten gebruikt met de 'fingerprints' (vooraf gedefinieerde herkenningsspatronen) van virussen, die worden opgesteld door gespecialiseerde securitybedrijven. Om nieuwe, nog niet-geïnterpreteerde virussen en spyware te kunnen herkennen in de bijlagen van e-mails, zijn heuristische (zelflerende) technieken nodig die (inhoudelijk) in bestanden kijken naar kwaadaardige code.¹⁰⁵

¹⁰⁰ Zie ook voetnoot 92.

¹⁰¹ Mondelinge inlichtingen Tele2 van 3 augustus 2012.

¹⁰² Daaronder begrepen de inhoud van door abonnees ontvangen en verzonden e-mails (inclusief attachments) aan de hand van vooraf gedefinieerde spam-, virus- en spywareherkenningsspatronen, voor zover nodig om spam en virussen/spyware tegen te houden en te verwijderen (oftewel, spam- en virusherkenningsgegevens uit de inhoud van het e-mailverkeer).

¹⁰³ Mondelinge inlichtingen Tele2 van 3 augustus 2012.

¹⁰⁴ In haar Fair Use policy schrijft Tele2 bijvoorbeeld mails te zullen weigeren als het onderwerp van de e-mail MAILER-DEAMON is.

¹⁰⁵ Een toelichting op virusbestrijdingstechnieken is te lezen op URL: http://en.wikipedia.org/wiki/Antivirus_software (website laatst bezocht op 15 juli 2012).

Informatie voor abonnees

De 'Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten' bevatten de volgende informatie over de verwerking van gegevens ten behoeve van spam-, virus- en spywarefiltering:

(...) Tele2 verzamelt en verwerkt (persoons)gegevens van de Klant voor zover deze nodig zijn voor een goede dienstverlening aan de Klant. Deze gegevens worden door Tele2 verwerkt en zonodig verstrekt aan derden, voor de volgende doeleinden:

a. de goede dienstverlening en de verdere ontwikkeling van de dienstverlening;

(...)

h. het voldoen aan wettelijk verplichtingen (...)."¹⁰⁶

Deze algemene voorwaarden bevatten een verwijzing naar de 'Fair Use Policy voor mobiele openbare elektronische communicatiediensten van Tele2'. Daarin staat:

"Tele2 mag in ieder geval ter behartiging van haar gerechtvaardigd belang e-mails zonder kennisgeving aan de afzender blokkeren en verwijderen in de volgende gevallen:

- als een attachment virus, spyware of andere schadelijke gegevens bevat;*
- als een attachment een op de website van Tele2 genoemde extensie heeft, zoals '.pif', '.scr', '.cmd', '.bat', and '.com';*
- de e-mail naar het oordeel van Tele2 kan leiden tot spamming of Mass Mailing;*
- de e-mail afkomstig is van een server/programma/virus die spam e-mails genereert;*
- als het onderwerp van de e-mail MAILER-DEAMON is en afkomstig is van internet service providers of e-mail providers die inkomende e-mails van programma's of virussen weigeren;*
- als de e-mail afkomstig is van internet servers providers die op de RBL-black list staan;*
- als er meer dan 50 e-mails binnen 5 minuten worden verzonden;*
- Tele2 mag e-mails die in uw 'Junk Mail' folder zijn geplaatst na 15 dagen verwijderen. E-mails in uw prullenbak mogen door Tele2 na 5 dagen worden verwijderd."¹⁰⁷*

Tele2 had tot april 2013 geen algemene privacy-verklaring.¹⁰⁸

¹⁰⁶ Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten (versie geldig vanaf 1 september 2009). URL: http://www.tele2.nl/files/AV_Mobiel_Internet.pdf, tevens aangetroffen op URL: http://www.tele2.nl/files/Algemene_Voorwaarden_-_Mobiel_Internet.pdf (URLs laatst bezocht op 29 mei 2013).

¹⁰⁷ Fair Use Policy voor mobiele openbare elektronische communicatiediensten van Tele2 (geldig vanaf 1 mei 2011). URL: http://www.tele2.nl/files/Fair_Use_Policy_Mobiele_telefoondiensten-2011.pdf (URL laatst bezocht op 29 mei 2013).

¹⁰⁸ Zie ook voetnoot 92.

Getroffen maatregel

In april 2013 heeft Tele2 een (algemeen) Privacy Statement gepubliceerd op haar website.¹⁰⁹ Dit Privacy Statement bevat de volgende informatie over de gegevensverwerkingen voor spam-, virus- en virusfiltering:

"Beveiliging van het netwerk en aansluitingen van onze klanten

*Tele2 probeert het internet voor zichzelf en voor haar klanten zo veilig mogelijk te houden door de inzet van firewalls, spamfilters en virusscanners. [...] Om aansluitingen van onze klanten en ons netwerk te beschermen, wordt al het internetverkeer dat ons netwerk binnenkomt automatisch gefilterd. Wanneer, voor bijvoorbeeld e-mail, Tele2 vermoedt dat een bericht een virus bevat dan zullen we proberen het virus te verwijderen en het bericht alsnog af te leveren, tenzij dit spam betreft. Spam wordt door ons op netwerkniveau tegengehouden. Zie hiervoor ook onze Gedragsregels voor Internet of Fair Use Policy voor Mobiel Internet."*¹¹⁰

¹⁰⁹ Privacy Statement Tele2 (april 2013).

¹¹⁰ Idem.

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).¹¹¹ De Privacyrichtlijn regelt de verwerking van persoonsgegevens en de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, waaronder het recht op (bescherming van de) persoonlijke levenssfeer. Daarnaast gelden de bepalingen uit de richtlijn betreffende privacy en elektronische communicatie 2002/58/EG (e-Privacyrichtlijn) (geïmplementeerd in de Tw).¹¹² De e-Privacyrichtlijn regelt de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor gebruikers van openbare elektronische communicatiediensten.¹¹³ 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).¹¹⁴ Er is geen sprake van een *lex specialis*-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene.¹¹⁵ 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).¹¹⁶

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

¹¹¹ “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.

¹¹² Zie artikel 1, tweede lid, van de e-Privacyrichtlijn; zie ook overweging 12 van de e-Privacyrichtlijn.

¹¹³ Zie artikel 1, eerste lid, van de e-Privacyrichtlijn; zie ook overwegingen 4, 8 en 12 van de e-Privacyrichtlijn.

¹¹⁴ 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.”

¹¹⁵ 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).

¹¹⁶ Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 45.

gevallen dat de specifieke wetgeving niet valt onder het bereik van dit artikel 2, geldt de regel «bijzondere wet gaat voor algemene wet» echter niet. De Wbp geldt in deze gevallen immers naast de specifieke wetgeving. Alsdan heeft de Wbp dus een aanvullende werking, namelijk voor die onderdelen die niet door de bijzondere wetgeving worden gedekt. De Organisatiewet sociale verzekeringen 1997 en de Telecommunicatiewet zijn daar een voorbeeld van. De geheimhoudingsvoorschriften in de Organisatiewet sociale verzekeringen vormen dus een uitwerking van die in de Wbp. Wel is het zo dat de voorschriften van de Wbp daarmee niet als direct bindende normen in beeld komen, ze spelen enkel zijdelings een rol.”¹¹⁷

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*.¹¹⁸

¹¹⁷ Kamerstukken II 1999/2000, 26 410, nr. 7, p. 2. Zie in dezelfde zin Kamerstukken II 1997/98, 25 892, nr. 3, p. 177: “In § 4 van het Algemeen deel van de toelichting «Algemene normen en sectorale invulling» noemden wij twee modellen van aanvullende wetten: het eerste waarbij uitputtend de gegevensbescherming in een wet is geregeld en het tweede waarbij in aanvulling op de Wet bescherming persoonsgegevens nadere regels zijn gesteld. Wordt het eerste model gevolgd, dan wordt de toepasselijkheid van het onderhavige wetsvoorstel uitdrukkelijk uitgesloten. (...) Wordt het tweede model gevolgd, dan is de Registratiekamer op grond van het wetsvoorstel bevoegd.” Vgl. ook Kamerstukken II 1997/98, 25 892, nr. 3, p. 13: “Voor het overige zullen veel bijzondere wetten op onderdelen concretisering bevatten, gericht op de sector die zij regelen. Het gaat daarbij formeel om *leges speciales* die derogeren aan de bepalingen van dit wetsvoorstel, maar materieel om een sectorale invulling die moet worden beoordeeld tegen de achtergrond van deze algemene normen, mede gelet op het feit ook deze bijzondere wetten aan de richtlijn [95/46/EG, toevoeging door het CBP] zullen moeten voldoen voor zover zij geheel of ten dele communautair recht bestrijken. (...) In artikel 2 WPR is ervan uitgegaan dat bij wetten van het tweede model [te weten: een uitputtend, bijzonder (privacy-)regime, waarbij in de wet wordt vermeld dat de toepasselijkheid van de algemene regels geheel wordt uitgesloten] *de niet-toepasbaarheid van WPR steeds in deze laatste wet zelf is vastgelegd*. Het onderhavige wetsvoorstel kiest voor een continuering van dit systeem. Deze keuze brengt met zich dat ook bij eventuele toekomstige wetgeving bevattende een uitputtend regime voor de bescherming van persoonsgegevens in een bepaalde sector, het niet van toepassing zijn van de WBP in deze laatste wet zelf wordt vermeld. Deze keuze voorkomt vragen over de verhouding tussen verschillende wettelijke systemen”, (onderstreping toegevoegd door het CBP).

¹¹⁸ 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

Tele2, gevestigd te Amsterdam en kantoorhoudende te Diemen, Nederland, bepaalt de doeleinden van en de middelen voor de verwerking van persoonsgegevens bij het gebruik van data-analyse technieken op het dataverkeer over haar mobiele netwerk.¹¹⁹

Tele2 heeft zich, voor zover voor dit onderzoek van belang, op 8 april 2008 als verantwoordelijke gemeld bij het CBP. Uit de gegevens uit het Handelsregister, en de verklaring van Tele2 [VERTROUWELIJK]¹²⁰ volgt dat Tele2 bevoegd - en in staat - is om doel en middelen vast te stellen. Tele2 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.¹²¹

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 degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde

verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk voor de verwerking van de aanvullende persoonsgegevens die noodzakelijk zijn voor de werking van de dienst."

¹¹⁹ Vgl. Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 4.

¹²⁰ Idem.

¹²¹ 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"*.

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.¹²²

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking¹²³ hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of - gezien de context¹²⁴ waarin ze worden verwerkt - medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.¹²⁵ 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.¹²⁶ 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.¹²⁷ Als voorbeeld wordt in de wetsgeschiedenis bij de Wbp genoemd het telefoonnummer.¹²⁸

¹²² Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.

¹²³ Zie WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007 (hierna: WP29 136), 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.

¹²⁴ Vgl. idem, p. 11: Er is sprake van informatie 'betreffende' een persoon "wanneer, rekening houdende met alle omstandigheden van het precieze geval, gegevens worden gebruikt of waarschijnlijk zullen worden gebruikt met het doel een persoon te beoordelen, op een bepaalde wijze te behandelen of de status of het gedrag van die persoon te beïnvloeden", met andere woorden, het doel.

¹²⁵ Kamerstukken II 1997/98, 25 892, nr. 3, p. 46. Vgl. WP29 136: 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.

¹²⁶ Kamerstukken II 1997/98, 25 892, nr. 3, p. 46 en 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".

¹²⁷ Idem, p. 46-47.

¹²⁸ 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 Rb. Dordrecht 31 augustus 2004, NBSTRAF 2004, 422 over het GSM-nummer (MSISDN) als OPENBARE VERSIE Rapport definitieve bevindingen van 29 mei 2013

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.”¹²⁹

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 persoon¹³⁰ - redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.¹³¹ 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.¹³² Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke.¹³³ In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.¹³⁴

Beoordeling

Het CBP heeft in paragrafen 2.4 tot en met 2.6 van dit rapport (p. 19 e.v.) vastgesteld dat Tele2 in verschillende apparatuur en systemen ten minste de volgende combinaties van gegevens over en uit het dataverkeer van abonnees van haar dataverkeersdiensten (betrokkenen) verwerkt(e):

persoonsgegevens.

¹²⁹ Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

¹³⁰ 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.

¹³¹ Idem, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip ‘onevenredige inspanning’ opgemerkt: “Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen.” Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.

¹³² Idem, p. 48. Vergelijk ook WP29 136, p. 16: “Daarbij moet rekening worden gehouden met alle relevante factoren, zoals de kosten van identificatie, het beoogde doel van de verwerking, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico op organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen.”

¹³³ Kamerstukken II 1997/98, 25 892, nr. 3, p. 48-49.

¹³⁴ Idem, p. 49. Vergelijk ook: Registratiekamer 27 maart 1995, 95.V.029.

Netwerkbeheer en marktonderzoek [VERTROUWELIJK]

[VERTROUWELIJK: identifiers]
vooraf gedefinieerde app, protocol en service patronen: • IP-adres van-naar • overige app/ protocol/service herkenninggegevens, uit de inhoud van het dataverkeer
hostname (URL op hoofddomein)
gebruikte service/protocol
[VERTROUWELIJK]
Frequentie en duur
verbruikte datavolume

Prepaidverkeer ([VERTROUWELIJK])

[VERTROUWELIJK]
[VERTROUWELIJK]

Spam-, virus- en spywarefiltering uit het e-mailverkeer

e-mailadressen
headers
bijlagen (attachments)

Daarbij beschikt Tele2 over de NAW-gegevens en/of e-mailadressen van (een groot deel van) haar abonnees (zie ook p. 16 van dit rapport), op grond van hun contractuele relatie.

Het CBP heeft in paragraaf 2.4 van dit rapport (p. 19 e.v.) vastgesteld dat Tele2 voor het doeleinde netwerkbeheer en marktonderzoeksdoeleinden (versleutelde) [VERTROUWELIJK: identifier], gebruikte protocol en verbruikte datavolume vastlegt en bewaart op individueel persoonsniveau, althans geaggregeerd per abonnee. De [VERTROUWELIJK: apparatuur] legt *voor de duur van de datasessie* van een abonnee ook [VERTROUWELIJK: identifiers] vast, in niet-permanent (werk)geheugen.¹³⁵ Dit alles doet Tele2 om het data ge-/verbruik en netwerkgebruik van betrokkenen in kaart te brengen.

Gegevens 'betreffende' een persoon

Het (versleutelde) [VERTROUWELIJK: identifier], in combinatie met (technische) gegevens over het bezoek aan en gebruik van apps, websites en protocollen zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over zijn mobiele data ge-/verbruik).¹³⁶

Daarnaast zijn [VERTROUWELIJK: identifier(s)], in combinatie met (technische) gegevens over (het functioneren van het netwerk/toestel bij) het gebruik daarvan

¹³⁵ Zie ook zienswijze 1 Tele2, randnummer 36 [VERTROUWELIJK] en Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 3 [VERTROUWELIJK].

¹³⁶ Hieruit volgt informatie over het communicatiegedrag van de betrokkene, bijvoorbeeld het identificeren van heavy users (top subscribers), en soms ook de inhoud van de communicatie.

door een individuele betrokkene gegevens over een natuurlijke persoon. Tele2 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 faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed, het verlagen van de snelheid van de verbinding bij overschrijding van de *Fair Use Policy*¹³⁷, het wijzigen van de abonnementsprijzen voor bepaalde types toestellen en het analyseren van de inhoud van ontvangen en verzonden e-mails (inclusief attachments) op spam-, virus- en spyware-herkenningspatronen om spam en virussen/spyware tegen te houden en te verwijderen. De gegevens worden dus door Tele2 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.¹³⁸

Niet doorslaggevend is of Tele2 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, en die mogelijkheid is aanwezig.

In de wetsgeschiedenis bij de Wbp is in dat verband opgemerkt: *“Indien het daarentegen mogelijk is de gegevens te gebruiken bij voorbeeld om fraude op te sporen, dan is er sprake van persoonsgegevens. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken, ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt.”*¹³⁹ Tele2 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 contactgegevens (waaronder het (versleutelde) [VERTROUWELJK: identifier], 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 Tele2 direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).

¹³⁷ Of Tele2 een grondslag heeft voor de inzet van data-analyse technieken ten behoeve van (handhaving van) de fair use policy wordt/is niet door het CBP beoordeeld.

¹³⁸ 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).

¹³⁹ *Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.*

Postpaid abonnees

Ten aanzien van Tele2 abonnees met een postpaid data abonnement, geldt het volgende.

Het [VERTROUWELIJK: identifier] van een abonnee met een postpaid data abonnement is voor Tele2 identificerend omdat zij een koppeling(smogelijkheid) heeft tussen dit nummer en NAW-gegevens en/of e-mailadres(sen). Er kan dus een relatie tussen de gegevens worden gelegd.

Tele2 beschikt verder een koppeling(smogelijkheid) tussen de [VERTROUWELIJK: identifier] en (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen, dan wel [VERTROUWELIJK: identifier(s)] en (het functioneren van het netwerk gedurende) het gebruik van het netwerk door een individuele betrokkene.¹⁴⁰

Niet alleen beschikt Tele2 over de (in)direct identificerende gegevens over en uit het dataverkeer in haar databases/bestanden, ook heeft Tele2 [VERTROUWELIJK] ter zake kundige technici in dienst 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.¹⁴¹ Hieruit blijkt dat de inspanning die Tele2 moet verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is. Het (versleutelde) [VERTROUWELIJK: identifier] van een abonnee met een postpaid data abonnement is voor Tele2 identificerend omdat zij een koppeling(smogelijkheid) heeft tussen dit nummer en NAW-gegevens en/of e-mailadres(sen).

Het CBP neemt verder in aanmerking dat de verwerking van de gegevens volgens Tele2 ook voor de volgende twee doeleinden geschiedt/geschiedde):

- (i) het faciliteren van het bezoek aan en van gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed;
- (ii) het verwijderen van spam, virus en spyware uit inkomende en uitgaande e-mails.

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

In de opinie van de Artikel 29-werkgroep, het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders, over het begrip

¹⁴⁰ Ook hier kan een relatie tussen de gegevens worden gelegd.

¹⁴¹ "IT heeft een enorm belangrijke impact op de organisatie en daarmee ook op de eindklant. Zonder het toegewijde team van [VERTROUWELIJK] medewerkers, kunnen we bij Tele2 niet het verschil maken." Zie ook URL: <http://werkenbij.tele2.nl/afdelingen/> (URL laatst bezocht op 29 mei 2013). Tele2 [VERTROUWELIJK] had in 2011 gemiddeld [VERTROUWELIJK] medewerkers. URL: [VERTROUWELIJK] (URL laatst bezocht op 29 mei 2013). De [VERTROUWELIJK: apparatuur] bevindt zich fysiek in [VERTROUWELIJK]. [VERTROUWELIJK] Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2-4.

persoonsgegevens is in dat verband opgemerkt: *“In dergelijke gevallen waarin het doel van de verwerking impliceert dat personen worden geïdentificeerd, kan worden verondersteld dat de voor de verwerking verantwoordelijke over “redelijkerwijs in te zetten middelen” beschikt om de betrokkene te identificeren. Aan te voeren dat personen niet identificeerbaar zijn als het doel van de verwerking nu juist die identificatie is, komt neer op een contradictio in terminis. De informatie moet dan ook worden beschouwd als informatie betreffende identificeerbare personen, wat betekent dat voor de verwerking de regels inzake gegevensbescherming gelden.”*¹⁴² 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.¹⁴³

Om deze twee doeleinden te verwezenlijken moeten de verwerkte gegevens herleidbaar zijn tot de betrokken abonnees. De gegevensverwerking is (dan) mede gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

Prepaid abonnees

Ten aanzien van Tele2 abonnees met een prepaid data abonnement, geldt het volgende.

Tele2 heeft verklaard dat zij NAW-gegevens en/of e-mailadressen heeft van circa [VERTROUWELIJK] van het totaal aantal prepaid abonnees.¹⁴⁴

Ten aanzien van de prepaid abonnees van wie Tele2 NAW-gegevens en/of e-mailadressen heeft, beschikt Tele2 over een koppeling(smogelijkheid) tussen enerzijds respectievelijk het (versleutelde) [VERTROUWELIJK: identifier] en [VERTROUWELIJK: identifier(s)], gecombineerd met NAW-gegevens en/of e-mailadressen en anderzijds respectievelijk (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen en gegevens over (het functioneren van het netwerk bij) het gebruik van het netwerk door een individuele betrokkene. Er kan een relatie tussen de gegevens worden gelegd.

In de wetsgeschiedenis bij de Tw wordt over de identificeerbaarheid van prepaid abonnees opgemerkt: *“Niettemin beschikken aanbieders in veel gevallen - bijvoorbeeld naar aanleiding van acties waarbij prepaid bellers een bepaald gratis beltegoed kunnen verkrijgen waarbij de verstrekking van persoonsgegevens als vereiste is gesteld - wel degelijk over persoonsidentificerende gegevens betreffende prepaid bellers. Aan de hand van het nummer van de prepaid klant kan dan een relatie tussen verkeersgegevens en die persoonsidentificerende gegevens worden gelegd.”*¹⁴⁵

Ten aanzien van de prepaid abonnees van wie Tele2 geen NAW-gegevens en/of e-mailadressen heeft, beschikt Tele2 wel over ten minste het (versleutelde) [VERTROUWELIJK: identifier] [VERTROUWELIJK] en, gedurende een internet sessie,

¹⁴² WP29 136. Advies 4/2007 over het begrip persoonsgegevens, 20 juni 2007, p. 16-17.

¹⁴³ Idem, p. 22.

¹⁴⁴ Reactie Tele2 op verzoek om inlichtingen van 11 april 2012, p. 2.

¹⁴⁵ Kamerstukken II 2002/03, 28 851, nr. 7, p. 80.

[VERTROUWELIJK: identifier]. Tele2 heeft, zoals hiervoor (zie p. 39 van dit rapport) vastgesteld, ook ter zake kundige technici in dienst en de benodigde technische faciliteiten om de gegevens, zonder onevenredige inspanning, aan elkaar te koppelen of zo nodig via tussenstappen te herleiden naar de betrokken abonnee.

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29-werkgroep over het begrip persoonsgegevens is hierover opgemerkt: *“(…) dat hoewel identificatie door middel van de naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan de geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook van de gebruiker ervan. (…) Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van “persoonsgegevens” weerspiegelt ook dit feit”, (onderstreping toegevoegd door het CBP).*¹⁴⁶

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.”*¹⁴⁷

Zakelijke abonnees

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

Ook gegevens over eenmanszaken en bedrijven handelend onder een eigenaam worden als persoonsgegevens aangemerkt, wanneer die ook iets zeggen over het gedrag van de eigenaar.¹⁴⁸

¹⁴⁶ WP29 136. Advies 4/2007 over het begrip persoonsgegevens, 20 juni 2007, p. 14-15.

¹⁴⁷ HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

¹⁴⁸ 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, 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*

Gelet op het voorgaande zijn de in deze paragraaf genoemde gegevens van Tele2 abonnees met een (prepaid of postpaid) data abonnement op zichzelf (te weten: de [VERTROUWELIJK: identifier(s)]), in onderlinge combinatie of in samenhang met uit andere bron bekende informatie, persoonsgegevens als bedoeld in artikel 1, onder a, van de Wbp.

De persoonsgegevens (informatie) over het communicatiegedrag van betrokkenen zijn gegevens van gevoelige aard. Het in kaart brengen van het surfgedrag van een natuurlijk persoon maakt inbreuk op de persoonlijke levenssfeer.¹⁴⁹

Hashing

Alvorens de hashingmethode van Tele2 te beoordelen (oftewel, de vraag of er sprake is van herleidbaarheid van het versleutelde [VERTROUWELIJK: identifier]), licht het CBP het begrip 'hashen' kort toe.

Hashen is een wiskundige bewerking die van informatie (bijvoorbeeld tekst) een unieke hashcode maakt die altijd even lang is (bijvoorbeeld 128 bits). Het maakt daarbij niet uit hoe groot de oorspronkelijke tekst is.

Hashen kan op verschillende wijzen worden toegepast. Hashen wordt bijvoorbeeld gebruikt voor het beveiligen van wachtwoorden die zijn opgeslagen in een database. De juistheid van een ingevoerd wachtwoord kan worden gecontroleerd door de hashwaarde van de invoer te vergelijken met de hashwaarde van het wachtwoord zoals die reeds in de database is opgeslagen. Voor zo'n controle hoeft men het wachtwoord zelf niet te kennen.

Een voorwaarde om hashen te gebruiken als een technische waarborg ter beveiliging van persoonsgegevens als bedoeld in artikel 13 van de Wbp is dat de hashwaarde niet kan worden teruggerekend tot de oorspronkelijke waarde.

Dat een hashwaarde niet kan worden teruggerekend, betekent echter nog niet dat de oorspronkelijke waarde (het identificerende gegeven) niet kan worden achterhaald via andere methoden, bijvoorbeeld via een lijstaanval.¹⁵⁰

beschouwd als de verwerking van gegevens over identificeerbare personen, ook als sommige personen in de praktijk niet identificeerbaar zijn." Idem, p. 17.

¹⁴⁹ Vgl. WP29 185, Opinion 13/2011 on Geolocation services on smart mobile devices van 16 mei 2011. URL: http://www.cbppweb.nl/downloads_int/wp185_en.pdf (URL laatst bezocht op 29 mei 2013). Zie ook Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010 (z2010-00582), p. 34 e.v. URL: http://www.cbppweb.nl/downloads_rapporten/rap_2011_google.pdf (URL laatst bezocht op 29 mei 2013). Zie Bevindingen Onderzoek door het College bescherming persoonsgegevens (CBP) naar de verwerking van persoonsgegevens door Advance Concepts B.V. van 15 december 2009, p. 27 en 28, URL: http://cbppweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf (URL laatst bezocht op 29 mei 2013).

¹⁵⁰ Een lijstaanval is een methode om een hash te 'hacken' door het uitproberen van alle mogelijke invoermogelijkheden; dit is mogelijk als de oorspronkelijke waarde een beperkt aantal posities heeft, bijvoorbeeld een wachtwoord '1234'. Hoe langer de invoer, des te

OPENBARE VERSIE Rapport definitieve bevindingen van 29 mei 2013

Hashen is naar zijn aard niet bedoeld om gegevens te anonimiseren. Verantwoordelijken hashen identifiers (zoals unieke nummers), in plaats van deze los te knippen en te vernietigen om zo de (bijbehorende) gegevens te anonimiseren, in veel gevallen om gegevens per betrokken persoon door de tijd heen aan elkaar te kunnen blijven koppelen. Hierbij is van belang dat deze bijkomende gegevens (die per hash worden georganiseerd) kunnen leiden tot identificatie van betrokkenen, zeker als het gaat over verzamelingen door de tijd heen van gedrag per betrokken persoon. Om te bereiken dat geen sprake meer is van persoonsgegevens moeten gegevens zijn ontdaan van alle (in)direct identificerende kenmerken die het mogelijk maken om die gegevens te herleiden naar een individuele natuurlijke persoon. Na verwijdering van deze (in)direct identificerende gegevens, mag identificatie ook op andere wijze niet (meer) mogelijk zijn. Pas dan worden er geen persoonsgegevens meer verwerkt en is de Wbp niet (meer) van toepassing.

Dit impliceert dat het loskoppelen van (in)direct identificerende gegevens en de overige gegevens onomkeerbaar moet zijn en dat deze gegevens ook in een later stadium - eventueel met behulp van andere (bijkomende of nieuwe) gegevens of technieken - niet alsnog aan elkaar mogen kunnen worden gekoppeld waardoor wederom personen kunnen worden geïdentificeerd. Indien er een risico op heridentificatie blijft bestaan, dan dienen verantwoordelijken technische en organisatorische maatregelen te treffen om dit risico te managen. De Wbp blijft in dat geval echter van toepassing op de set gegevens.

In het Witboek voor beslissers van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt de toepassing van privacy enhancing technologies (PET) toegelicht.

PET is de verzamelnaam voor een aantal technieken die de verantwoordelijke kan toepassen om bij het verwerken van persoonsgegevens de risico's voor de betrokkenen te beperken.

Uit het Witboek blijkt dat het scheiden van gegevens als een vorm van pseudonimiseren moet worden opgevat, en niet als een vorm van anonimiseren. Het Witboek definieert scheiding van gegevens als volgt: *"Splitsing van identiteitsdomein en pseudo-identiteitsdomein. Identiteitsbeschermer onder beheer gegevensverwerkende organisatie of TTP of betrokkenen in geval persoonsgegevens in eigen beheer wordt toegepast."*¹⁵¹ De indeling in dit rapport wordt ook aangehaald in de recente CBP Richtsnoeren beveiliging van persoonsgegevens. *"Van anonimisering is sprake als de gegevens op geen enkele manier meer tot de betrokkene te herleiden zijn. Er is dan geen sprake meer van persoonsgegevens en de Wbp is niet meer van toepassing op de gegevens. Een lichtere vorm van*

moeilijker is een lijstaanval. Een toelichting op 'woordenlijstaanval' is te lezen op: URL: <http://nl.wikipedia.org/wiki/Woordenlijstaanval> (website laatst bezocht op 5 april 2013).

¹⁵¹ Drs. Ing. Ronald Koorn RE e.a., *Privacy Enhancing Technologies, Witboek voor beslissers*, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, december 2004, p. 41. URL: http://www.cbpreb.nl/downloads_technologie/witboek_pet.pdf (URL laatst bezocht op 29 mei 2013).

PET is het scheiden van de verwerkte persoonsgegevens in (zeer goed beveiligde) identificerende gegevens en niet-identificerende gegevens.”¹⁵²

Beoordeling

Identificatie zonder de naam van de abonnee en/of heridentificatie door Tele2 via [VERTROUWELIJK]
[VERTROUWELIJK]

Daardoor kan Tele2 de [VERTROUWELIJK: identifiers] behorende bij de (her)berekende unieke hashwaarden achterhalen.¹⁵³

Tele2 [VERTROUWELIJK] heeft een groot aantal ter zake kundige technici in dienst en beschikt over (toegang tot) de benodigde technische faciliteiten.¹⁵⁴ Er is heridentificatie mogelijk. Hieruit volgt dat de inspanning die Tele2 [VERTROUWELIJK] moet verrichten om de gegevens over en uit het dataverkeer naar een individuele natuurlijke persoon te (kunnen) herleiden (oftewel, het ‘omzeilen’ van de technische maatregel) niet onevenredig is. De gebruikte hashingmethode leidt (aldus) niet tot onomkeerbare anonimisering van de verwerkte gegevens.

Ontleuteling door Tele2 [VERTROUWELIJK] via [VERTROUWELIJK]
[VERTROUWELIJK]

De [VERTROUWELIJK] waarborgen leiden er niet toe dat geen sprake meer is van persoonsgegevens.

Uit het voorgaande blijkt dat ontsleuteling door Tele2 [VERTROUWELIJK] (via [VERTROUWELIJK: B] en/of [VERTROUWELIJK: A]), en door [VERTROUWELIJK: B] en/of [VERTROUWELIJK: A] (‘voor zichzelf’) mogelijk is. Het ‘omzeilen’ van deze organisatorische maatregel vergt geen onevenredige inspanning van Tele2 [VERTROUWELIJK], en [VERTROUWELIJK: B] en/of [VERTROUWELIJK: A]. De gebruikte hashingmethode leidt (aldus) niet tot onomkeerbare anonimisering van de verwerkte gegevens over en uit het dataverkeer.

¹⁵² CBP Richtsnoeren beveiliging van persoonsgegevens, 19 februari 2013, p. 10, URL: http://www.cbpreb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf (URL laatst bezocht op 29 mei 2013).

¹⁵³ Dit geldt temeer daar een 06-nummer uit maximaal 10 posities bestaat, en dat slechts een beperkt gedeelte van de potentiële nummerreeksen aan Tele2 is toebedeeld, de nummerreeks 06-3600 tot en met 06-4099. URL: <https://www.acm.nl/nl/onderwerpen/telecommunicatie/telefoonnummers/nummers-doorzoeken/resultaat/?query=&bestemming=061%2C+062%2C+063%2C+064%2C+065%2C+068+-+Mobiele+nummers&status=Toegekend&relatie=Tele2&datum=> (URL laatst bezocht op 29 mei 2013).

¹⁵⁴ “IT heeft een enorm belangrijke impact op de organisatie en daarmee ook op de eindklant. Zonder het toegewijde team van [VERTROUWELIJK] medewerkers, kunnen we bij Tele2 niet het verschil maken.” URL: <http://werkenbij.tele2.nl/afdelingen/> (URL laatst bezocht op 29 mei 2013). Tele2 [VERTROUWELIJK] had in 2011 gemiddeld [VERTROUWELIJK] medewerkers. URL: [VERTROUWELIJK] (URL laatst bezocht op 29 mei 2013). De [VERTROUWELIJK: apparatuur] bevindt zich fysiek in [VERTROUWELIJK] in [VERTROUWELIJK]. Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 2-4.

Tele2 schrijft in haar zienswijze 2 dat uit de overwegingen van de Artikel 29-werkgroep in advies 4/2007 over het begrip persoonsgegevens blijkt "(i) dat gebruik van niet-geaggregeerde statistische gegevens zo kan worden ingericht dat geen sprake is van persoonsgegevens, (ii) dat hashing daarbij een rol kan spelen, en (iii) dat bij de beoordeling of heridentificatie mogelijk is, de waarschijnlijkheid daarvan moet worden meegewogen en niet kan worden volstaan met het identificeren van theoretische mogelijkheden tot heridentificatie."¹⁵⁵ De door Tele2 toegepaste hashing is volgens Tele2 een vorm van eenrichtingsversleuteling die in beginsel leidt tot anonieme data waarop de Wbp niet langer van toepassing is.¹⁵⁶ Tele2 haalt voorbeeld 17 uit de betreffende opinie aan (non-aggregated data for statistics) waaruit blijkt dat (via een sleutel) herleidbare gegevens in sommige gevallen voor de ontvanger geen persoonsgegevens zijn, afhankelijk van de getroffen waarborgen. "In dat kader wijst Tele2 erop dat het advies op p. 21 ook uitdrukkelijk de toepassing van onomkeerbare hashing noemt als een voorbeeld van een passende technische maatregel om identificatie te voorkomen. Is daarvoor gekozen, maar is desondanks door onvoorziene omstandigheden toch heridentificatie mogelijk, dan is dat volgens de Art. 29 Groep geen reden om alle gehashte informatie als persoonsgegevens te beschouwen, nu heridentificatie niet redelijkerwijs te verwachten was."¹⁵⁷

In algemene zin is bij inschakeling van een TTP/onafhankelijke derde die een cryptografische sleutel bewaart of een cryptografische module beheert sprake van een beveiligingsmaatregel van gegevensscheiding. In beginsel is gegevensscheiding een passende beveiligingsmaatregel, maar gegevensscheiding betekent niet dat de betreffende gegevens niet meer gelden als persoonsgegevens. Alleen in uitzonderlijke omstandigheden, zoals de waarborg van een medisch beroepsgeheim, kan een dergelijke gegevensscheiding ertoe leiden dat niet langer sprake is van persoonsgegevens voor de ontvanger. Het gaat hier echter niet om beoordeling van de resultante van de hashing voor de ontvanger, maar om de beoordeling of het voor Tele2 (nog) persoonsgegevens zijn. Er is de facto geen sprake van onomkeerbare anonimisering, omdat Tele2 [VERTROUWELIJK], en daarbij komende gegevens vastlegt over het gebruik van protocollen, (geselecteerde) apps en bezoek aan (geselecteerde) hostnames. [VERTROUWELIJK]. Het doeleinde van de verwerking door Tele2 is gericht op het waarnemen en vastleggen van individueel gedrag door de tijd heen. Het gaat dus niet om een onvoorziene omstandigheid, zoals bedoeld in de door Tele2 aangehaalde opinie van de Artikel 29-werkgroep. De gegevensverwerking is mede gericht op individualisatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

Voorgestelde maatregelen

Op verzoek van het CBP heeft Tele2 een offerte aangevraagd bij haar leverancier [VERTROUWELIJK] (zie p. 24 van dit rapport).

De door Tele2 voorgestelde mogelijkheden om [VERTROUWELIJK] leiden evenmin tot onomkeerbare anonimisering. [VERTROUWELIJK]. Door deze werkwijze blijft Tele2 in staat om het gedrag per klant door de tijd heen te volgen, en telkens nieuwe gegevens over en uit het dataverkeer aan de [VERTROUWELIJK] hashwaarde per

¹⁵⁵ Zienswijze 2 Tele2 van 30 oktober 2012, randnummer 43. Zie **bijlage IV** bij dit rapport.

¹⁵⁶ Idem, randnummer 45.

¹⁵⁷ Idem, randnummer 47.

klant te koppelen. Wil er sprake zijn van daadwerkelijk onomkeerbare anonimisering, dan dient Tele2 de persoonsgegevens direct uit de datastroom te verwijderen en aldus de gegevens te aggregeren tot een niveau waarop ze niet meer in verband kunnen worden gelegd met individuele klanten. Uit technisch onderzoek blijkt¹⁵⁸ en Tele2 geeft desgevraagd aan dat een dergelijke oplossing technisch mogelijk is [VERTROUWELIJK].¹⁵⁹

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 bij de traditionele spraaktelefonienetwerken. Dit is relevant voor de tenuitvoerlegging van de richtlijn.”*¹⁶⁰

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

¹⁵⁸ [VERTROUWELIJK].

¹⁵⁹ [VERTROUWELIJK].

¹⁶⁰ 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.).

door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren zij ook tot de verkeersgegevens. Verkeersgegevens kunnen o.a. gegevens zijn met betrekking tot de routing, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop communicatie begint of eindigt, het begin, het einde of de duur van de verbinding (...)"¹⁶¹

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

Of sprake is van persoonsgegevens die tevens verkeersgegevens zijn, is afhankelijk van het doel van de verwerking, te weten: voor het overbrengen van communicatie of voor andere doelen.¹⁶²

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."*¹⁶³

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 communicatie¹⁶⁴ zijn gegevens die ook bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8

¹⁶¹ 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.

¹⁶² W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?', *Computerrecht* 2003, p. 28.

¹⁶³ *Kamerstukken II 2007/08*, 31 145, nr. 9, p. 16-17.

¹⁶⁴ *"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).

van het Handvest van de grondrechten van de Europese Unie (Handvest).¹⁶⁵ Het Europees Hof voor de Rechten van de Mens (EHRM) oordeelde in zijn arrest van 3 april 2007 over de bescherming van e-mailcorrespondentie en internetgebruik: *“Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8”*, (onderstreping toegevoegd door het CBP).¹⁶⁶

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.”*¹⁶⁷

Beoordeling

De begripsafbakening tussen ‘communicatie’ en ‘verkeersgegevens’ wordt bemoeilijkt door de steeds sterkere vervlechting van de gevoerde communicatie en de daarmee samenhangende gegevens in de technische protocollen. Bij spraaktelefonie kan het onderscheid tussen deze begrippen nog worden gemaakt langs de lijn van de 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 wetsgeschiedenis¹⁶⁸ geeft een indicatie welke categorieën van gegevens over het dataverkeer als verkeersgegevens moeten worden aangemerkt. Beide noemen onder andere de routing, de duur, het tijdstip, het volume van de communicatie, het gebruikte protocol en de locatiegegevens als gegevens die door het netwerk waarover de

¹⁶⁵ 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/hm/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.cbppweb.nl/Pages/adv_z2012-00746.aspx (URL laatst bezocht op 29 mei 2013).

¹⁶⁶ EHRM 3 april 2007, NJ 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44.

¹⁶⁷ 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 (...)”*

¹⁶⁸ 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.

communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen.

Ook ten aanzien van de hostname (URL op hoofddomein) geldt dat deze door het netwerk waarover de communicatie wordt doorgegeven, wordt 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).

De verkeersgegevens over het communicatiegedrag van betrokkenen (URL's en apps) zijn gegevens van gevoelige aard.¹⁶⁹ 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.”*¹⁷⁰ En: *“Het gaat niet om het opslaan van websites die zijn bezocht.”*¹⁷¹ De Wet bewaarplicht telecommunicatiegegevens vormt een implementatie van de richtlijn betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten 2006/24/EG (Dataretentierichtlijn). Artikel 1, tweede lid, van de Dataretentierichtlijn luidt: *“Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Zij is niet van toepassing op de inhoud van elektronische communicatie, de informatie die wordt geraadpleegd met behulp van een elektronisch communicatienetwerk daaronder begrepen.”* Artikel 5, tweede lid, van de Dataretentierichtlijn bepaalt: *“Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mogen krachtens deze richtlijn niet worden bewaard.”*

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

Deze kenmerken worden herkend in de initiatiefase van het protocol.

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

¹⁶⁹ Kamerstukken II 2000/01, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.

¹⁷⁰ Kamerstukken I 2008/09, 31 145, C, p. 17. Zie in dezelfde zin idem, p. 12.

¹⁷¹ Handelingen II 2007/08, 83, p. 5836.

worden vervoerd die gegevens uit de applicatielaag bevatten, betekent niet dat die pakketten dus communicatiegegevens bevatten.

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

(Louter) gegevens uit het dataverkeer zijn communicatie tevens persoonsgegevens. Ten aanzien van spam-, virus- en malwareherkenningsgegevens uit (gedownloade) bestanden en verzonden en ontvangen e-mails geldt, voor zover Tele2 deze verwerkt om spam en malware/virussen tegen te houden en te verwijderen, dat geen sprake is van verkeersgegevens, maar van zulke communicatie (de bestanden en berichten die worden overgebracht).¹⁷²

Samengevat, kunnen de persoonsgegevens worden ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals [VERTROUWELIJK: identifiers], de starttijd en eindtijd van de data sessie, verbruikte datavolume, protocollen, hostnames, etc.
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

3.5 Gegevensverwerking

Uitwerking van het wettelijk kader

Het begrip ‘verwerking van persoonsgegevens’ als bedoeld in artikel 1, onder b, van de Wbp omvat het gehele proces dat een persoonsgegeven doormaakt vanaf het moment van verzamelen tot aan het moment van vernietiging.¹⁷³ Ook het genereren van persoonsgegevens is een verwerking.¹⁷⁴ Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze gegevens.¹⁷⁵ 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).¹⁷⁶ Een telecomoperator die enkel gegevens doorvoert zonder

¹⁷² Het CBP heeft bovenstaande toepassing van de begrippen ‘communicatie’ en ‘verkeersgegevens’ voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom – College bescherming persoonsgegevens van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van deze begrippen in dit rapport.

¹⁷³ Zie *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 51-52.

¹⁷⁴ *Idem*, p. 51

¹⁷⁵ 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.

¹⁷⁶ Met dien verstande dat de desbetreffende handelingen met betrekking tot verkeersgegevens van abonnees die geen natuurlijke personen zijn niet zonder meer persoonsgegevens zijn.

daarop enige invloed uit te kunnen oefenen (*mere conduit*), verwerkt daarmee geen persoonsgegevens.¹⁷⁷

Beoordeling

Het CBP heeft in paragrafen 2.4 en 2.5 (p. 19 e.v. van dit rapport) vastgesteld dat Tele2 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). Tele2 verwerkt (aldus) persoonsgegevens die (in de meeste gevallen) ook verkeersgegevens zijn. Er is dus geen sprake van een *mere conduit*-uitzondering. Tele2 verkrijgt (verzamelt) de persoonsgegevens via het gebruik van data-analyse technieken. De persoonsgegevens worden ofwel aangemaakt in haar mobiele netwerk (dataverbruik gegevens om te kunnen factureren), ofwel Tele2 inspecteert gegevens in de headers [VERTROUWELIJK] (ordering van al aanwezige gegevens).¹⁷⁸

Het CBP heeft in paragraaf 2.4 van dit rapport (p. 19 e.v. van dit rapport) vastgesteld dat Tele2 voor het doeleinde netwerkbeheer en marktonderzoeksdoeleinden in de [VERTROUWELIJK: apparatuur] persoonsgegevens opslaat van al haar abonnees. Tele2 bewaart de met behulp van deze data-analyse apparatuur vastgelegde persoonsgegevens, voor zover de doeleinden van de gegevensverwerking binnen de scope van dit onderzoek vallen, gedurende ten hoogste twaalf maanden.¹⁷⁹

Gelet op het voorgaande verwerkt Tele2 persoonsgegevens als bedoeld in artikel 1, onder b, van de Wbp.

3.6 Grondslag

Uitwerking van het wettelijk kader

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

Artikel 5 van de e-Privacyrichtlijn bepaalt (kort gezegd), voor zover voor dit onderzoek van belang: de lidstaten verbieden het af luisteren, 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.

¹⁷⁷ Idem: “Zodra er enige feitelijke macht over persoonsgegevens is, is het wetsvoorstel van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking kunnen onder de wettelijke regeling vallen. Cruciaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige) invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend. Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing”, (onderstreping toegevoegd door het CBP). Idem, p. 51-52.

¹⁷⁸ Idem, p. 68.

¹⁷⁹ Reactie Tele2 op verzoek om inlichtingen van 19 september 2011, p. 3: [VERTROUWELIJK]

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.¹⁸⁰

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, af luisteren of anderszins onderscheppen of controleren van de communicatie via een openbaar elektronisch communicatienetwerk of openbare elektronische communicatiedienst en de daarmee verband houdende gegevens tenzij en voor zover:*

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

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

In de wetsgeschiedenis bij artikel 11.2a is opgemerkt over *Deep Packet Inspection* (hierna: DPI): *“Artikel 11.2a Tw ziet op de vertrouwelijkheid van de communicatie die via internet of andere elektronische communicatiediensten of -netwerken plaats vindt. Dit artikel waarborgt aldus dat de vertrouwelijkheid van de communicatie van bedrijven en consumenten, bijvoorbeeld via internet, wordt gewaarborgd. Overigens verbiedt artikel 11.2a Tw in den brede het aftappen of af luisteren, en dergelijke van communicatie door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, dus ook wanneer dit plaats heeft met een andere methode dan de methode van Deep Packet Inspection. Bezien vanuit de positie van de aanbieders van elektronische communicatienetwerken en diensten stellen beide artikelen grenzen aan het beheer van de door hen aangeboden netwerken en diensten. Belangrijk op te merken is dat zowel artikel 7.4a als artikel 11.2a Tw (zie met name tweede lid, onder b en c) er niet aan in de weg staan dat een aanbieder zijn netwerk en diensten op een «normale» manier beheert. Zo mag, ook in het kader van artikel 11.2a Tw (zie tweede lid, onder c), een aanbieder van een netwerk om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht*

¹⁸⁰ Kamerstukken I 2011/12, 32 549, E, p. 2.

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).¹⁸¹

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.”*¹⁸²

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.”*¹⁸³

¹⁸¹ Kamerstukken I 2011/12, 32 549, E, p. 13.

¹⁸² Kamerstukken I 2011/12, 32 549, F, p. 5.

¹⁸³ Kamerstukken II 2010-2011, 32 549, nr. 16, p. 2-3.

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:*
 - 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 zijn toestemming heeft gegeven. (...)¹⁸⁴*
- 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

¹⁸⁴ 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.

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.¹⁸⁵ Voor dataverkeer is dit bijvoorbeeld afhankelijk van het type dienst.¹⁸⁶

Onder het begrip ‘anonimiseren’ wordt verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken.¹⁸⁷ 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.¹⁸⁸ Het kan nodig zijn dat er andere, aanvullende maatregelen worden getroffen om herleidbaarheid van de gegevens te voorkomen.

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

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

Facturering, verkeersbeheer en behandeling van verzoeken om inlichtingen van abonnees

De (Europese) wetgever heeft beoogd het begrip ‘facturering’ een ruime betekenis te geven. Onder de verwerking ten behoeve van de facturering wordt niet alleen het opstellen van een factuur begrepen, maar ook bijvoorbeeld het registreren van het beltegoed van prepaid abonnees (en betaling van verleende toegang).¹⁸⁹ In de wetsgeschiedenis bij de Tw wordt daarover opgemerkt: *“Daarmee komt ook buiten kijf te*

¹⁸⁵ Kamerstukken II 2002/03, 28 851, nr. 3, p. 154.

¹⁸⁶ 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.

¹⁸⁷ Idem, nr. 7, p. 80.

¹⁸⁸ Kamerstukken II 1997/98, 25 892, nr. 3, p. 48.

¹⁸⁹ Kamerstukken II 2002/03, 28 851, nr. 3, p. 155.

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 belang; dit laatste dient onder facturering te worden begrepen."¹⁹⁰

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).¹⁹¹ Het gaat hier niet om zelfstandige verwerkingsdoeleinden, maar om verwerkingsdoeleinden die van het factureringsdoeleinde en het doeleinde het overbrengen van de communicatie zijn afgeleid.¹⁹² De verkeersgegevens mogen (ook) voor die (afgeleide) doeleinden worden verwerkt, voor zover noodzakelijk.

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

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" (...)." ¹⁹³

Het Hof van Justitie van de EG vult het begrip noodzakelijkheid, 'een autonoom begrip van gemeenschapsrecht', op een strikte wijze in.¹⁹⁴ 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 gegevens op naam te bewaren en te verwerken.¹⁹⁵

¹⁹⁰ Idem, nr. 13, p. 20.

¹⁹¹ Idem, nr. 3, p. 156.

¹⁹² Idem.

¹⁹³ EHRM 25 maart 1983, nr. 97 (Silver & Others v. United Kingdom).

¹⁹⁴ Vgl. ook HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 52.

¹⁹⁵ HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 64-65 en 68: "Ebenzo 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."

Ten aanzien van de verwerking ten behoeve van de facturering geldt dat het noodzakelijkheids criterium nader wordt ingevuld doordat is bepaald dat de verwerking is toegestaan tot het einde van de termijn waarbinnen de factuur in rechte kan worden betwist dan wel de betaling in rechte kan worden afgedwongen.¹⁹⁶ 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 doeleinde te bewaren.¹⁹⁷

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).¹⁹⁸

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."*¹⁹⁹

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*

¹⁹⁶ Kamerstukken II 2002/03, 28 851, nr. 3, 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).

¹⁹⁷ Idem.

¹⁹⁸ Het CBP heeft bovenstaande uitleg van artikel 11.5 van de Tw voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom – College bescherming persoonsgegevens van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van dit artikel in dit rapport.

¹⁹⁹ Kamerstukken II 2002/03, 28 851, nr. 7, p. 54. Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 6.

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.²⁰⁰

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.²⁰¹ ‘Specifiek’ betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).²⁰² ‘Geïnformeerd’ betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.²⁰³

Van *ondubbelzinnige* toestemming is slechts sprake indien bij de verantwoordelijke elke twijfel is uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.²⁰⁴ ‘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).²⁰⁵ 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

²⁰⁰ 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.

²⁰¹ *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.

²⁰² *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. 41. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (URL laatst bezocht op 29 mei 2013).

²⁰³ *Idem.*

²⁰⁴ *Idem.*, p. 80.

²⁰⁵ *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.

betrokkene daartoe ondubbelzinnig zijn toestemming heeft gegeven, enkel omdat hij de betreffende overeenkomst heeft ondertekend.”²⁰⁶

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.”²⁰⁷

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.²⁰⁸ Daarbij geldt als voorwaarde dat het moet gaan om een overeenkomst waarbij de betrokkene partij is²⁰⁹ en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (dat wil zeggen: als de overeenkomst niet goed kan worden uitgevoerd zonder de persoonsgegevens).²¹⁰

De uitgever van een krant mag bijvoorbeeld de persoonsgegevens van zijn abonnees verwerken omdat dat noodzakelijk is om de krant te kunnen bezorgen²¹¹ (zonder NAW-gegevens van de betreffende betrokkene kan bezorging niet plaatsvinden).

De verwerking kan niet worden gebaseerd op deze grondslag als de verwerking nuttig zou zijn of de uitvoering van een overeenkomst zou vergemakkelijken, maar niet echt noodzakelijk is aangezien er een manier bestaat om de overeenkomst uit te voeren zonder de persoonsgegevens (proportionaliteits- en subsidiariteitstoets).²¹² De

²⁰⁶ *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.

²⁰⁷ WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 41.

²⁰⁸ *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80.

²⁰⁹ *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.

²¹⁰ *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 81.

²¹¹ *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).

²¹² 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).

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*.²¹³ 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.²¹⁴ 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).²¹⁵ Anders gezegd: er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.²¹⁶ Daarbij moet onder andere worden gelet op de aard van de in het geding zijnde taak en de aard van de betrokken persoonsgegevens.²¹⁷ 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.²¹⁸ 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.²¹⁹

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 verrichten²²⁰) of van een derde aan wie

²¹³ 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.”

²¹⁴ 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.

²¹⁵ *Idem*, p. 82-83. Een verwerking die uitsluitend dient ter uitvoering van een wettelijk recht valt hier buiten.

²¹⁶ *Idem*, p. 82.

²¹⁷ *Idem*, p. 83.

²¹⁸ *Idem*.

²¹⁹ *Idem*.

²²⁰ *Idem*, p. 86.

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).²²¹

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.²²² 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.²²³

Uit de wetsgeschiedenis bij de Wbp kan wel worden afgeleid dat artikel 8 van de Wbp een uitputtende opsomming geeft van verwerkingsgronden: *“Artikel 7 betreft de verzameling van persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Hierop zijn geen uitzonderingen. Hetzelfde geldt voor de in artikel 8 genoemde gronden op basis waarvan persoonsgegevens mogen worden verwerkt. Artikel 8 omvat derhalve een uitputtende opsomming van verwerkingsgronden.”*²²⁴

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

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp²²⁵ op het punt van de bevoegdheid tot (toelaatbaarheid van) het bewaren van persoonsgegevens die ook verkeersgegevens zijn (oftewel, een verplichting tot

²²¹ 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.

²²² *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 87.

²²³ Idem.

²²⁴ *Kamerstukken II* 1998/99, 25 892, nr. 13, p. 5-6.

²²⁵ Te weten: het vereiste dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

verwijdering dan wel anonimisering van gegevens, met uitzonderingen).²²⁶ 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).²²⁷ Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp.

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

Persoonsgegevens die ook communicatie betreffen

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

Artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) geeft een verplichting voor de aanbieder van een openbare elektronische communicatiedienst en -netwerk om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Dit artikel 11.3 van de Tw stelt eisen aan de beveiliging van persoonsgegevens en geeft aldus een telecomspecifieke

²²⁶ 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.

²²⁷ 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.

uitwerking van artikel 13 van de Wbp.²²⁸ Het artikel geeft (dus) geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

Als hoofdregel geldt op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het 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 overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder. Het artikel geeft echter op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens (maar uitzonderingen op het verwerkingsverbod).

Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.3 en/of artikel 11.2a van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Dat daargelaten, geeft de regeling in artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en (richtlijnconforme uitleg van)²²⁹ 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. Dat betekent materieel (inhoudelijk) dat als de gegevensverwerking is toegestaan onder artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw; dat wil zeggen: uit dit artikel een wettelijke plicht voortvloeit) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw; dat wil zeggen: uit dit artikel een verwerkings-/uitzonderingsgrond voortvloeit) ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw ook geen grondslag is te vinden in de Wbp (waarbij dit laatste artikel 8 van de Wbp in de toets materieel (inhoudelijk) dan enkel zijdelings een rol speelt).

²²⁸ 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.

²²⁹ 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*).

Beoordeling

3.6.1 Netwerkbeheer en marktonderzoeksdoeleinden

Het CBP heeft in paragraaf 2.4 van dit rapport (p. 19 e.v.) vastgesteld dat Tele2 een [VERTROUWELIJK: identifier] in combinatie met gegevens over het bezoek aan en gebruik van apps, websites en protocollen genereert/verzamelt en gebruikt, vastlegt en gedurende twaalf maanden bewaart om inzicht te hebben/krijgen in welke soorten diensten (apps/websites etc.) welke hoeveelheid capaciteit innemen op de verschillende delen van het netwerk.

Het CBP heeft in paragrafen 3.1 tot en met 3.4 van dit rapport (p. 32-50) beoordeeld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Tele2 stelt in haar zienswijze dat zij zich voor netwerkbeheer (en marktonderzoeksdoeleinden) baseert op het verwerkingsdoeleinde verkeersbeheer.²³⁰

Als hoofdregel geldt sinds 1 januari 2013 (en voorheen in artikel 5 van de ePrivacyrichtlijn) op grond van artikel 11.2a van de Tw dat het af luisteren, 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-analyse-technieken zulke gegevens wil verzamelen voor de in artikel 11.2a van de Tw genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Activiteiten tot behoud/verbetering van de netwerk performance of de dienstverlening van de mobiele aanbieder (waaronder netwerkplanning) *kunnen*,

²³⁰ Zienswijze 1 Tele2, randnummer 59.

mede gelet op de wetsgeschiedenis bij artikel 11.2a van de Tw, in beginsel onder het verwerkingsdoel verkeersbeheer vallen (mits er een proportionele implementatie is).²³¹ Het CBP neemt in aanmerking dat Tele2 aangeeft de data-analysetechnieken slechts in beperkte mate in te zetten. [VERTROUWELIJK].

Hieruit volgt dat er een beperkte noodzaak is voor Tele2 om gegevens over het dataverkeer op deze niet-geanonimiseerde wijze te inspecteren/genereren (verzamelen) om de benodigde informatie te hebben/(kunnen) krijgen (verzamelen) over (het volume van) datagebruik als gevolg van (de toename van) het gebruik van allerlei protocollen, apps en websites.

Tele2 heeft aannemelijk gemaakt dat er, gegeven de huidige stand van de techniek, geen andere manieren en minder ingrijpende middelen beschikbaar zijn (zoals marktonderzoek) om hetzelfde resultaat te bereiken.

De noodzaak om (een beperkte set) gegevens over het dataverkeer te verzamelen behelst niet zonder meer een noodzaak om de aldus verkregen gegevens vervolgens ook op individueel niveau vast te leggen en gedurende twaalf maanden te bewaren. Getoetst moet worden of ook deze verwerking voldoet aan het proportionaliteits- en subsidiariteitsvereiste. Dat wil zeggen, of het doeleinde niet anderszins of met minder ingrijpende middelen worden bereikt en of de inbreuk op de belangen van de bij de verwerking betrokkenen evenredig is in verhouding tot het met de verwerking te dienen doel.

De aard van de verzamelde persoonsgegevens, de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor gegevensvergarig in de vorm van data-analyse technieken naar aanleiding van het gebruik van het netwerk van de aanbieders en het risico (kans x impact) voor de betrokkenen van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, spelen een rol in de belangenafweging. Daarnaast worden de inspanning en kosten meegewogen die voor Tele2 gepaard gaan met de ontwikkeling en implementatie van (technische) mogelijkheden om hetzelfde doel op een andere, minder inbreukmakende wijze te bereiken, evenals de consequenties voor de continuïteit en integriteit van haar netwerk.

Tele2 stelt dat het voor netwerkbeheer noodzakelijk is om dataverbruik te kunnen waarnemen op individueel niveau, door de tijd heen, om trends te kunnen waarnemen en te kunnen anticiperen op veranderingen in het dataverkeer over tijd. Deze informatie kan aanleiding zijn om de netwerkcapaciteit uit te breiden, of te bezien of de beprijzing van datadiensten moet worden aangepast.

Tele2 schrijft: *“Verwijdering van persoonsgegevens leidt praktisch gezien tot aggregatie van informatie. Dat zou ertoe leiden dat Tele2 nog wel kan zien dat er in augustus 2012 15.483 keer gebruik is gemaakt van een nieuwe voice-over-IP app op het netwerk van Tele2, en dat dit*

²³¹ Vgl. o.a. *Kamerstukken I 2011/12*, 32 549, E, p. 13 over het beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is de diverse verkeersstromen die over dat netwerk worden afgewikkeld in kaart brengen.

in oktober is toegenomen tot 133.788 keer, maar niet of het daarbij gaat om dezelfde abonnees die de betreffende app steeds vaker gebruiken of een toename in het aantal abonnees dat de app gebruikt. Evenmin is zichtbaar of dat gebruik per abonnee over tijd toeneemt, afneemt of stabiel blijft.”²³²

Tele2 stelt dat zij terughoudend gebruikt maakt van de [VERTROUWELIJK: apparatuur] technologie, voor beperkte doelen, en dat haar werkwijze, gegeven de getroffen waarborgen, daarom voldoet aan de eisen van proportionaliteit en subsidiariteit.

Het CBP begrijpt dat het voor het netwerkbeheer van Tele2 handig kan zijn om individueel gedrag door de tijd heen te kunnen volgen, maar daarmee is de gevolgde specifieke data-analyse methode met behulp van de [VERTROUWELIJK]-apparatuur niet automatisch ook noodzakelijk en daarmee gerechtvaardigd.

[VERTROUWELIJK]. Om vast te stellen of bepaalde types toestellen meer datagebruik veroorzaken dan anderen hoeft Tele2 derhalve geen persoonsgegevens vast te leggen en te bewaren. Ten aanzien van individueel gebruik van specifieke protocollen, apps en websites heeft Tele2 onvoldoende onderbouwd en aannemelijk gemaakt waarom het voor haar noodzakelijk zou zijn voor netwerkbeheer om onderscheid te kunnen maken tussen het gedrag van individuele gebruikers. Immers, ongeacht de vraag of 1 gebruiker honderd keer per dag naar een specifieke website of app gaat, of dat honderd gebruikers dat 1 maal per dag doen, heeft Tele2 voldoende capaciteit nodig op haar netwerk om dit verkeer te kunnen overbrengen. Indien het aantal dagelijkse bezoeken aan een website of app steeds toeneemt, kan Tele2 een inschatting maken van benodigde netwerkcapaciteit of andere door haar genoemde mogelijke interventie maatregelen treffen, zoals [VERTROUWELIJK]. Dergelijke ontwikkelingen met betrekking tot het datavolume kunnen heel goed uit geaggregeerde gegevens worden opgemaakt.

Daarbij komt dat Tele2 in haar zienswijze zelf aangeeft alleen geaggregeerde gegevens nodig te hebben om de benodigde informatie te hebben/(kunnen) krijgen over de netwerkbelasting: [VERTROUWELIJK].

Het CBP verwijst - nu de door Tele2 voor netwerkbeheer verwerkte gegevens uitsluitend worden gebruikt voor kwantitatief statistisch en technisch onderzoek - ook naar het 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 doel niet noodzakelijk is om de gegevens op naam te bewaren en te verwerken.²³³

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

²³² Zienswijze 2 Tele2, randnummer 24. Zie **Bijlage IV** bij dit rapport.

²³³ HvJ EG 16 december 2008, EHRC 2009, 23. (LJN BG7811; Huber), r.o. 52. Vgl AG HvJ 3 april 2008, zaak C-524/06 (Huber), r.o. 23: "Statistieken zijn per definitie anoniem en niet persoonsgebonden."

wijze moeten worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt.

Het CBP stelt vast dat de bij Tele2 in gebruik zijnde [VERTROUWELIJK]-apparatuur technisch in staat is om de persoonsgegevens:

- (i) onomkeerbaar te ontdoen van [VERTROUWELIJK: identifier]
- (ii) te pseudonimiseren door de [VERTROUWELIJK: identifier] in niet-persistent (werk)geheugen te hashen en vervolgens het versleutelde [VERTROUWELIJK: identifier] met de (bijkomende) gegevens over het bezoek aan en gebruik van apps, websites, protocollen op te slaan in de achterliggende databases/bestanden.

Uit het onderzoek is gebleken dat huidige bij Tele2 in gebruik zijnde [VERTROUWELIJK]-apparatuur technisch ook in staat is om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren (zie p. 44-45 van dit rapport). Door het aanpassen van de configuratie-instellingen kunnen de [VERTROUWELIJK: identifiers] onomkeerbaar verwijderd worden uit de gegevens. Dit in plaats van de huidige hashing methode die op de [VERTROUWELIJK: identifiers] wordt toegepast.

Hetzelfde doel, het verkrijgen van verkeersstatistieken voor netwerkbeheer, kan dus op een andere, minder inbreukmakende wijze worden bereikt.

Ten aanzien van de risico's voor betrokkenen dat er op inbreuk wordt gemaakt op hun persoonlijke levenssfeer geldt het volgende. 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 oneigenlijk gebruik van gegevens te voorkomen, (beveiligings)incidenten niet altijd kunnen worden voorkomen. Het hashen van het [VERTROUWELIJK: identifier] is wel een waarborg ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp. Maar gelet op de aard van de verzamelde persoonsgegevens bieden andere maatregelen dan het zo snel 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.

Omdat de huidige werkwijze van Tele2 niet voldoet aan de vereisten van proportionaliteit en subsidiariteit is van een noodzaak voor het gebruiken, vastleggen en bewaren van persoonsgegevens over het dataverkeer voor het doeleinde van netwerkbeheer geen sprake. Omdat Tele2 ook geen ander noodzakelijk verwerkingsdoeleinde heeft voor de onder dit kopje besproken gegevensverwerking, handelt Tele2 in strijd met artikel 11.5 van de Tw. Hierdoor kan van een grondslag als genoemd in artikel 8 van de Wbp ook geen sprake zijn en handelt Tele2 eveneens in strijd met artikel 8 van de Wbp.

Marktonderzoeksdoeleinden

Uit artikel 11.5, derde lid, van de Tw volgt dat verkeersgegevens alleen mogen worden verwerkt voor marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten als de betrokkene daarvoor zijn toestemming heeft gegeven. Zo'n verwerkingsdoel correspondeert - mogelijk - met de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp). Tele2 heeft niet verklaard en uit het onderzoek is ook overigens niet gebleken dat Tele2 daadwerkelijk om (ondubbelzinnige) toestemming heeft gevraagd en die toestemming is verkregen.

Volgens Tele2 gebruikt zij de gegevens niet voor gerichte marketing naar klanten, maar voor algemene analyses, die ertoe leiden dat zij bijvoorbeeld de abonnementsvoorwaarden kan aanpassen. Tele2 maakt daarmee een onderscheid tussen direct marketing (verkoopactiviteiten) en marktonderzoek (ten behoeve van het bepalen van de prijsstelling van bestaande producten en diensten, en het ontwikkelen van nieuwe diensten). Artikel 11.5, derde lid, van de Tw vereist echter toestemming van de betrokkenen voor zowel marktonderzoek als verkoopactiviteiten met betrekking tot elektronische communicatiediensten.

Omdat van toestemming niet is gebleken, kan Tele2 zich niet beroepen op artikel 11.5, derde lid, van de Tw. Door het ontbreken van een noodzakelijk verwerkingsdoel in artikel 11.5 van de Tw kan van een grondslag als genoemd in artikel 8 van de Wbp geen sprake zijn en handelt Tele2 dus in strijd met artikel 11.5, derde lid, van de Tw, jo. artikel 8 van de Wbp.

3.6.2 Prepaidverkeer

Het CBP heeft in paragraaf 2.5 van dit rapport (p. 28 e.v.) vastgesteld dat Tele2 [VERTROUWELIJK].

Het CBP heeft in paragraaf 3.3 van dit rapport (p. 34 e.v.) vastgesteld dat dit een verwerking is van persoonsgegevens die tevens verkeersgegevens zijn.

Zoals vermeld in de uitwerking van het wettelijk kader, geldt als hoofdregel op grond van artikel 11.5, eerste lid, van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer noodzakelijk zijn ten behoeve van (het doel van) de overbrenging van communicatie. Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor

facturering). Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Als de gegevensverwerking is toegestaan onder artikel 11.5 van de Tw is ook een bijbehorende grondslag te vinden als opgesomd in artikel 8 van de Wbp (waarbij dit laatste artikel in de toets materieel (inhoudelijk) enkel zijdelings een rol speelt) en - omgekeerd - als de verwerking niet is toegestaan onder de Tw is ook geen grondslag te vinden in de Wbp.

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

Uit de wetsgeschiedenis bij de Tw volgt dat het verwerkingsdoel facturering 'ruim' dient te worden opgevat in de zin dat verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed (dit laatste dient onder facturering te worden begrepen).²³⁴

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

Tele2 stelt in haar zienswijze dat zij zich voor het routeren van verkeer naar opwaardeersites voor opwaardering baseert op de noodzaak van het uitvoeren van een overeenkomst. Tele2 heeft van de prepaidklant opdracht gekregen om tegen vooruitbetaling toegang te verlenen tot internet, en zonder mogelijkheid van gratis opwaardering zou de prepaidklant verstoken zijn van verder gebruik van mobiel internet als zijn tegoed op is. Dit correspondeert, bij nader inzien van het CBP, met het verwerkingsdoel facturering.²³⁵ De wijze waarop Tele2 de data-analyse voor dit doeleinde inzette, was in deze context een proportionele implementatie van het bieden van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed, gelet op de omstandigheid dat Tele2 [VERTROUWELIJK] en de verwerkte gegevens niet bewaarde.

²³⁴ Kamerstukken II 2002/03, 28 851, nr. 13, p. 20.

²³⁵ Zienswijze 1 Tele2, randnummers 74 en 77-78.

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

Getroffen maatregel

Bij brief van 11 april 2012, in reactie op het rapport Voorlopige Bevindingen, heeft Tele2 aangegeven dat geen gebruik meer wordt gemaakt van de [VERTROUWELIJK] data-analyse apparatuur om prepaid abonnees in staat te stellen gratis hun tegoed op te waarderen.²³⁶ Indien Tele2 de data-analyse apparatuur weer inzet op de wijze die door het CBP is onderzocht en beoordeeld, is geen sprake van een overtreding.

3.6.3 Spam-, virus- en spywarefiltering van e-mailverkeer

Het CBP heeft in paragraaf 2.6 (p. 29 van dit rapport) vastgesteld dat Tele2 e-mailadressen in combinatie met spam-, virus- en malwareherkenningsgegevens uit de inhoud van het e-mailverkeer van betrokkenen inspecteert/verzamelt en gebruikt om spam, virussen en spyware te blokkeren en te verwijderen.

Het CBP heeft in paragraaf 3.3 (p. 34 e.v. van dit rapport) vastgesteld dat dit een verwerking van persoonsgegevens die ook communicatie betreffen is.

Zoals vermeld in de uitwerking van het wettelijk kader, geldt als hoofdregel op grond van (richtlijnconforme uitleg van) artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers verboden is, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan. Dit artikel geeft aldus een verwerkingsverbod, met uitzonderingen. Op deze eerder genoemde hoofdregel is in lid 2 van artikel 11.2a van de Tw bijvoorbeeld een uitzondering geformuleerd voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder. Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de genoemde (uitgezonderde) doeleinden, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Het artikel geeft echter op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens (maar uitzonderingen op het verwerkingsverbod). Als de gegevensverwerking is toegestaan onder artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) is ook een bijbehorende grondslag te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw is ook geen grondslag te vinden in de Wbp (waarbij dit laatste artikel 8 van de Wbp in de toets materieel (inhoudelijk) dan enkel zijdelings een rol speelt).

²³⁶ Brief Tele2 van 11 april 2012, p. 2.

Tele2 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, kan naar het oordeel van het CBP ook het aanbieden van virusfilters voor inkomende en eventueel uitgaande e-mails worden begrepen en het bestrijden van spyware. Filtering van uitgaande spam kan naar het oordeel van het CBP ook noodzakelijk zijn voor Tele2 om deze wettelijke plicht uit te voeren.²³⁷

Het CBP heeft in paragraaf 2.6 (p. 29 van dit rapport) vastgesteld dat internet aanbieders ook naar de inhoud van verzonden en ontvangen e-mails inclusief bijlagen moeten kijken om spam/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 spam- (bij uitgaande spam), virus- en malwareherkenningsgegevens noodzakelijk is voor (de uitvoering van) de zorgplicht internetveiligheid.²³⁸

Uit het voorgaande blijkt dat Tele2 een grondslag heeft voor deze verwerking van persoonsgegevens die ook communicatie betreffen onder artikel 11.3 van de Tw jo. artikel 8 van de Wbp. Op basis van het beschikbare onderzoeksmateriaal heeft het CBP ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens die ook communicatie betreffen geen overtreding geconstateerd van artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp.

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

²³⁷ In de opinie van de Artikel 29-werkgroep is in 2006 opgemerkt dat filtering van (inkomende) spam onder omstandigheden kan worden gebaseerd op de grondslag uitvoering van een overeenkomst en/of wettelijke plicht (vgl. artikel 8, aanhef en onder b en c, van de Wbp). WP29 118. Advies 2/2006 over de privacyaspecten van e-mailscreeningdiensten, p. 6. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_nl.pdf (URL laatst bezocht op 29 mei 2013).

²³⁸ Idem: p. 5-6 over de zorgplicht van internet- en e-mailproviders.

kan het generiek filteren van inkomende spam nuttig zijn omdat klanten dit op prijs stellen en omdat het onnodige belasting van netwerken en systemen voorkomt. Artikel 7.4a, eerste lid, onderdeel c, stelt hiervoor wel als voorwaarde dat de abonnee toestemming heeft gegeven. De aanbieder die alleen generiek op spam wil filteren, zou ervoor kunnen kiezen om bij het afsluiten van een overeenkomst te wijzen op het nut van een spamfilter en het geven van toestemming als voorwaarde voor het sluiten van de overeenkomst te stellen.”²³⁹

Het Samenwerkingsprotocol CBP-OPTA (zijnde werkafspraken tussen de verschillende toezichthouders binnen de grenzen van de onderscheidene wetten waarin hun bevoegdheden zijn geregeld) regelt/geeft onder andere bepalingen over de behandeling bij samenlopende bevoegdheden en de uitwisseling en verstrekking van informatie tussen de ACM²⁴⁰ en het CBP. Op grond van artikel 2, tweede en derde lid, van het Samenwerkingsprotocol CBP-OPTA zal de ACM zich bij het uitoefenen van haar bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van de bepalingen van de Tw ligt en zal het CBP zich bij het uitoefenen van zijn bevoegdheden primair richten op gevallen waar het zwaartepunt in de toepassing van bepalingen van de Wbp ligt. Het beoordelen van (de toelaatbaarheid van) het filteren op inkomende spam ligt volgens de toezichthouders vanaf de inwerkingtreding van artikel 7.4a van de Tw meer op de weg van de ACM.²⁴¹ De inzet van data-analyse technieken vanaf 1 januari 2013 voor het filteren op inkomende spam valt daarom buiten de scope van dit onderzoek.

3.7 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.²⁴²

‘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).²⁴³ Het doeleinde mag

²³⁹ Kamerstukken I 2011/12, 32 549, G, p. 8.

²⁴⁰ De ACM is krachtens artikel 42, zesde lid, van de Instellingswet Autoriteit Consument en Markt in dit Samenwerkingsprotocol CBP-OPTA per [1 april 2013] in de plaats getreden van OPTA.

²⁴¹ Vgl. ook de taakverdeling ten aanzien van spam (artikel 5 van het Samenwerkingsprotocol CBP-OPTA). Het artikel geeft op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens, maar uitzonderingen op het verwerkingsverbod.

²⁴² Kamerstukken II 1997/98, 25 892, nr. 3, p. 79.

²⁴³ Idem.

ook niet in de loop van het verzamelproces worden geformuleerd.²⁴⁴ '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.²⁴⁵

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."*²⁴⁶

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 paragrafen 2.4 tot en met 2.6 van dit rapport (p. 19 e.v. van dit rapport) vastgesteld dat Tele2 persoonsgegevens verzamelt/verwerkt bij de inzet van data-analyse technieken in haar mobiele netwerk.

Tele2 heeft als doeleinden van de gegevensverwerking geformuleerd, voor zover deze binnen de scope van dit onderzoek vallen: netwerkbeheer en marktonderzoeksdoeleinden, spam-, virus- en spywarefiltering van e-mailverkeer en (tot april 2012) het afhandelen van verkeer van prepaidklanten naar opwaardeersites .

In paragraaf 3.9 van dit rapport (p. 79 e.v. van dit rapport) wordt beoordeeld dat de doelomschrijving onvoldoende duidelijk is in de meldingen die Tele2 heeft gedaan.

Het CBP heeft in paragraaf 2.1 van dit rapport (p. 13 e.v. van dit rapport) vastgesteld dat Tele2 geen andere meldingen heeft gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele netwerk.

De in deze paragraaf bedoelde verwerkingen van persoonsgegevens voldoen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens niet aan de eisen die worden gesteld aan de categorieën van vrijgestelde verwerkingen die zijn beschreven in de artikelen van het Vrijstellingsbesluit Wbp.²⁴⁷ De verwerkingen van persoonsgegevens zijn daarom niet

²⁴⁴ Idem.

²⁴⁵ Idem.

²⁴⁶ Idem.

²⁴⁷ De enige artikelen die mogelijksterwijs 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 OPENBARE VERSIE Rapport definitieve bevindingen van 29 mei 2013

vrijgesteld van de melding.²⁴⁸ Tele2 heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp, waardoor de meldingen bij die functionaris zouden kunnen zijn gedaan (artikel 27, derde lid, van de Wbp).

Doordat Tele2 de hiervoor genoemde drie doeleinden waarvoor zij persoonsgegevens verwerkt(e) onvolledig en onvoldoende duidelijk heeft omschreven bij de meldingen die Tele2 heeft gedaan, zijn/worden de door Tele2 verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelt Tele2 in strijd met artikel 7 van de Wbp.

Het CBP heeft in de paragraaf 3.6.1 (p. 64 e.v. van dit rapport) vastgesteld dat Tele2 niet in alle stadia van de verwerking een grondslag heeft voor de gegevensverwerkingen voor de doeleinden netwerkbeheer en marktonderzoek.

Doordat de gegevensverwerkingen voor de doeleinden netwerkbeheer en marktonderzoek niet in alle stadia kunnen steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, worden de door Tele2 verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelt Tele2 in strijd met artikel 7 van de Wbp.

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.²⁴⁹

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.

²⁴⁸ 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.*"

²⁴⁹ 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

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.²⁵⁰

Deze bepaling vormt een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing'.²⁵¹ 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.²⁵² 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.²⁵³

Artikel 34 van de Wbp gaat er vanuit dat er geen onderzoeksplicht van de betrokkene is.²⁵⁴

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

c. de duur van het aftappen, af luisteren, onderscheppen of controleren van de gegevens. Deze informatieplicht is in dit geval niet relevant omdat de toestemmingsuitzondering op het verwerkingsverbod van artikel 11.2a, tweede lid, onder a van de Tw niet aan de orde is.

²⁵⁰ *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 149-150.

²⁵¹ *Idem*, p. 149.

²⁵² *Idem*.

²⁵³ *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*.

²⁵⁴ *Idem*, p. 150.

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 het verwerkingsdoel verkeersbeheer is 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 de paragrafen 2.4 en 2.5 (p. 19 e.v. van dit rapport) vastgesteld dat Tele2 persoonsgegevens die ook verkeersgegevens zijn verwerkt voor de doeleinden netwerkbeheer en marktonderzoek en (tot april 2012) verwerkte voor het afhandelen van verkeer van prepaidklanten naar opwaardeersites.

Het CBP heeft in paragraaf 3.3 (p. 34 e.v. van dit rapport) vastgesteld dat Tele2 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.

Hetzelfde geldt voor spam-, virus- en malwareherkenningsgegevens uit de inhoud van het e-mailverkeer. Het CBP heeft in paragraaf 2.6 (p. 29 e.v. van dit rapport) vastgesteld dat Tele2 deze persoonsgegevens die ook communicatie betreffen verwerkt voor het doeleinde van spam-, virus en spywarebestrijding in het e-mailverkeer.

Het CBP heeft in de paragrafen 3.3 en 3.4 (p. 34 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 het verwerkingsdoel verkeersbeheer is afgeleid van het factureringsdoel, moet Tele2 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. Op grond hiervan moet Tele2 de betrokkenen onder andere de doeleinden van de verwerking mededelen en nadere informatie geven voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is.

In de 'Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten' wordt louter opgemerkt, zonder dit nader te specificeren of toe te lichten: *"Tele2 verzamelt en verwerkt (persoons)gegevens [daaronder mede begrepen verkeersgegevens, toevoeging door het CBP] van de Klant voor zover deze nodig zijn voor een goede dienstverlening aan de Klant. Deze gegevens worden door Tele2 verwerkt en zonodig verstrekt aan derden, voor de volgende doeleinden:*

*a. de goede dienstverlening en de verdere ontwikkeling van de dienstverlening; (...)
e. netwerkbeheer en de bevordering van een efficiënte inrichting van de bedrijfsprocessen;
f. marktonderzoek- en direct marketingdoeleinden; (...)"*²⁵⁵

De ratio van de informatieplicht is dat de burger in staat moet zijn te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.²⁵⁶

Tele2 informeert betrokkenen via deze algemene voorwaarden niet over de soorten verkeersgegevens die voor netwerkbeheer en marktonderzoekdoeleinden worden verwerkt en niet over de soorten verkeersgegevens die werden verwerkt ten behoeve van het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed.

Tele2 informeert betrokkenen via haar 'Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten' niet over de doeleinden en duur van de gegevensverwerking. Oftewel, niet over de verwerking van persoonsgegevens (waaronder hostnames en apps) voor de doeleinden netwerkbeheer en marktonderzoek en het gedurende twaalf maanden bewaren van deze gegevens op individueel niveau en (tot april 2012) voor het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed.

Tele2 had, voor zover voor dit onderzoek van belang²⁵⁷, tot april 2013 geen algemene privacy-verklaring.

Wel informeert Tele2 via haar 'Fair Use Policy voor mobiele openbare elektronische communicatiediensten van Tele2' over haar beleid met betrekking tot het bestrijden van spam, virussen en spyware in e-mails.

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 gegevensvergaring²⁵⁸ in de vorm van data-analyse technieken) en het gebruik dat ervan wordt/werdgemaakt, is het nodig dat Tele2 de betrokkenen nadere informatie verstrekt over de categorieën van verwerkte

²⁵⁵ Algemene Voorwaarden Tele2 voor Mobiele Internet Diensten (versie geldig vanaf 1 september 2009). URL: http://www.tele2.nl/files/AV_Mobiel_Internet.pdf, tevens aangetroffen op URL: http://www.tele2.nl/files/Algemene_Voorwaarden_-_Mobiel_Internet.pdf (URLs laatst bezocht op 29 mei 2013).

²⁵⁶ *Kamerstukken II 1997/98, 25 892, nr. 3, p. 149.*

²⁵⁷ Het toepassingsbereik van de Privacy Policy van Tele2 was: "voor bezoekers van de websites die via <http://www.tele2.nl> toegankelijk zijn." URL: <http://www.tele2.nl/algemeen/privacy-policy.html> (URL laatst bezocht op 4 maart 2013).

²⁵⁸ Vgl. *Kamerstukken II 1997/98, 25 892, nr. 3, p. 78.*

gegevens²⁵⁹ en de bewaartermijn teneinde tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen.²⁶⁰

Mededeling van de informatie aan de betrokkenen via een privacyverklaring/algemene voorwaarden op de Tele2 website was mogelijk en betekende geen onevenredige inspanning.

Het CBP heeft in paragraaf 3.6 (p. 51 e.v. van dit rapport) vastgesteld dat de *vastlegging* van de persoonsgegevens niet bij of krachtens de wet is/was voorgeschreven.

Doordat Tele2 de betrokkenen niet uiterlijk op het moment van vastlegging van de hen betreffende persoonsgegevens informeerde over de soorten persoonsgegevens die zij verwerkt voor de doeleinden netwerkbeheer en marktonderzoek handelde Tele2 (in ieder geval tot april 2013) in strijd met artikel 11.5, vierde lid, van de Tw, jo. artikel 34 van de Wbp.²⁶¹

Doordat Tele2 de betrokkenen evenmin informeerde over de soorten persoonsgegevens die zij verwerkte tot april 2012 voor het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed, handelde Tele2 tot april 2012 eveneens in strijd met artikel 11.5, vierde lid, van de Tw, jo. artikel 34 van de Wbp.

Voorgestelde maatregel

Tele2 heeft bij haar tweede zienswijze een voorstel gevoegd om de informatie aan betrokkenen uit te breiden. Tele2 noemde daarin een bewaartermijn van 12 maanden voor de gegevens en kwam daarmee ten dele tegemoet aan de door het CBP geconstateerde tekortkomingen in de informatie aan betrokkenen. De beknopte omschrijving bevatte echter geen informatie over de soorten verkeersgegevens die Tele2 verwerkt. De mededeling dat gegevens [VERTROUWELIJK] worden opgeslagen, was onvoldoende begrijpelijk. Invoering van deze voorgestelde maatregel had niet tot beëindiging geleid van de geconstateerde overtreding van artikel 11.5, vierde lid, van de Tw, jo. artikel 34 van de Wbp.

Getroffen maatregel

In april 2013 heeft Tele2 voor het eerst een algemene privacy-verklaring gepubliceerd.

In haar Privacy Statement (versie april 2013) informeert Tele2 betrokkenen dat zij data-analysetechnieken inzet voor de planning en het beheer van haar mobiele datanetwerk. Tele2 verklaart met behulp van die technieken voor dat doelinde gegevens te verzamelen en te verwerken met betrekking tot het gebruik van de mobiele datadiensten. Tele2 informeert daarbij over de categorieën van verwerkte

²⁵⁹ Vgl. ook artikel 11, eerste lid, onder c, van de Privacyrichtlijn.

²⁶⁰ 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).

²⁶¹ 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 tevens leidt tot onrechtmatige verwerking(en). *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 149.

persoonsgegevens die ook verkeersgegevens zijn (onder het kopje 'Internetgegevens'). Onder het kopje 'Inzet van data-analyse techniek' wordt opgemerkt: "*Hiertoe worden gegevens verzameld zoals het toesteltype en de apps die je gebruikt, de bezochte webdomeinen, en het dataverbruik op een bepaald moment.*" Aanvullend informeert Tele2 betrokkenen (nu ook via het Privacy Statement) dat zij firewalls, spamfilters en virusscanners gebruikt om het internet voor zichzelf en haar klanten zo veilig mogelijk te houden.

Door deze informatie heeft Tele2 de geconstateerde overtreding van artikel 11.5, vierde lid, van de Tw, jo. artikel 34 van de Wbp, deels beëindigd.

Tele2 merkt onder het kopje '(Direct) marketing- en verkoopdoeleinden' op dat zij verkeersgegevens gebruikt "*om op geaggregeerd niveau (d.w.z. dat deze gegevens niet worden herleid naar individuele personen) analyses te kunnen maken van het bel-, internet- en kijkgedrag van onze klanten.*" De zinsnede 'dat deze gegevens niet **worden** herleid naar individuele personen' is onvolledig en onvoldoende duidelijk, omdat ze wel herleidbaar **zijn** (zie hierover verder het kopje 'Marktonderzoekdoeleinden', p. 68 van dit rapport).

Voorts informeert Tele2 betrokkenen via haar Privacy Statement alleen in abstracto over bewaartermijnen: "*Tele2 streeft ernaar gegevens niet langer te bewaren dan noodzakelijk. Dat betekent bijvoorbeeld dat we gegevens waarmee de factuur is berekend, vernietigen of anonimiseren zodra de factuur is voldaan.*" En: "*Deze gegevens worden per klant in geanonimiseerde vorm opgeslagen voor analyse ten behoeve van netwerkbeheer. Hierbij wordt niet naar de inhoud van het verkeer gekeken.*" Dit is onvoldoende specifiek. De zinsnede in het nieuwe Privacy Statement dat 'de gegevens per klant in geanonimiseerde vorm worden opgeslagen' moet als feitelijk onjuist worden aangemerkt, althans is onvolledig en onvoldoende duidelijk (zie hierover verder paragraaf 3.3, onder het kopje 'Hashing', p. 42 van dit rapport).

Doordat de duur van de verwerking (bewaartermijnen) en het doeleinde van de verwerking voor marktonderzoekdoeleinden onvolledig en onvoldoende duidelijk zijn vermeld in het Privacy Statement van Tele2, duurt de overtreding van artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp op deze punten voort.

3.9 Meldingsplicht

Uitwerking van het wettelijk kader

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

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

Beoordeling

Het CBP heeft in paragraaf 3.7 van dit rapport (p. 72 e.v. van dit rapport) vastgesteld dat Tele2 de doeleinden - samengevat weergegeven - netwerkbeheer en marktonderzoeksdoeleinden, filtering van e-mailverkeer voor spam, virus en spywarebestrijding en (tot april 2012) het faciliteren van het bezoek aan en gebruik van (gratis) opwaardeersites bij een ontoereikend prepaid tegoed waarvoor zij persoonsgegevens verwerkt niet had gemeld, dan wel onvolledig en onvoldoende duidelijk heeft (had) omschreven in de doelomschrijving in de meldingen die zij heeft gedaan met nummers m1249952 en m1252089.

Het CBP heeft in paragraaf 2.1 van dit rapport (p. 13 e.v.) vastgesteld dat Tele2 geen andere meldingen heeft gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele netwerk. De in deze paragraaf bedoelde verwerkingen van persoonsgegevens voldoen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens niet aan de eisen die worden gesteld aan de categorieën van vrijgestelde verwerkingen die zijn beschreven in de artikelen van het Vrijstellingsbesluit Wbp.²⁶² De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding.²⁶³ Tele2 heeft geen functionaris gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.

Doordat Tele2 deze verwerkingen van persoonsgegevens niet heeft gemeld bij het CBP, handelt Tele2 in strijd met artikel 27 jo. 28 van de Wbp.

Voorgestelde maatregel

Zoals beschreven in paragraaf 2.1 (p. 13 e.v. van dit rapport) heeft Tele2 een concept wijziging van de melding toegestuurd aan het CBP.²⁶⁴ Daarin meldt Tele2 als doeleinden enerzijds het analyseren en de opslag van geanonimiseerde gegevens ten behoeve van netwerkbeheer en anderzijds het verwerken van mobiel dataverkeer om het in geanonimiseerde vorm te analyseren en op te slaan. Tele2 geeft daarnaast inzicht in de soorten persoonsgegevens die zij vervolgens opslaat.

Uit de beoordeling van de toegepaste hashing methode bij de data-analyse voor het doeleinde van netwerkbeheer (paragraaf 3.3, onder het kopje 'Hashing', p. 42 van dit rapport) volgt dat de gegevens niet onomkeerbaar zijn geanonimiseerd. Bij de verwerking van gegevens uit het e-mailverkeer ten behoeve van spam, virus en spywarebestrijding is geen sprake van enige vorm van anonimisering.

Tele2 maakt in de concept wijziging van de melding onvoldoende duidelijk wat het verschil is tussen de twee doeleinden (analyseren en opslaan van geanonimiseerde gegevens versus verwerken om vervolgens in anonieme vorm op te slaan en te analyseren). Het CBP mist daarbij bovendien de doeleinden van marktonderzoek en van spam-, virus- en spywarebestrijding in het e-mailverkeer.

²⁶² Zie voetnoot 246.

²⁶³ Zie voetnoot 247.

²⁶⁴ Zienswijze 2 Tele2, bijlage 2 – (Concept) Meldingsformulier Wbp.

Ten slotte heeft Tele2 de vraag niet beantwoord of er sprake is van doorgifte van persoonsgegevens naar landen buiten de Europese Unie.

Omdat de concept gewijzigde melding bij het CBP onvolledig is en onvoldoende duidelijk, leidt deze, ook na de daadwerkelijke invoering ervan, in deze vorm niet tot beëindiging van de geconstateerde overtreding van artikel 27, jo. 28 van de Wbp.

3.10 Bewerkerovereenkomst

Uitwerking van het wettelijk kader

Artikel 14 van de Wbp bepaalt dat de uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke. Artikel 1, aanhef en onder e, van de Wbp bepaalt: *een bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.*

De verantwoordelijke draagt zorg dat de bewerker de persoonsgegevens slechts verwerkt in opdracht van de verantwoordelijke en passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (artikel 14 jo. 12, eerste lid, en 13 van de Wbp).

Dit artikel 14 van de Wbp vormt een implementatie van artikel 17, tweede tot en met vierde lid, van de Privacyrichtlijn:

(...)

2. De Lid-Staten bepalen dat de voor de verwerking verantwoordelijke, in geval van verwerking te zijnen behoeve, een verwerker moet kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking en moet toezien op de naleving van die maatregelen.

3. De uitvoering van verwerkingen door een verwerker moet worden geregeld in een overeenkomst of een rechtsakte die de verwerker bindt jegens de voor de verwerker verantwoordelijke en waarin met name wordt bepaald dat

- de verwerker slechts handelt in opdracht van de voor de verwerking verantwoordelijke,
- de in lid 1 bedoelde verplichtingen, zoals gedefinieerd door de wetgeving van de Lid-Staat waarin de verwerker is gevestigd, eveneens op deze persoon rusten.

4. Met het oog op de bewaring van de bewijzen, worden de elementen van de overeenkomst of rechtsakte betreffende de bescherming van de gegevens en de vereisten inzake de in lid 1 bedoelde maatregelen schriftelijk of in een gelijkwaardige vorm vastgelegd.

Bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder dat hij diens ondergeschikte is. Bepalend voor de afbakening van het begrip bewerker is de relatie met de verantwoordelijke voor de gegevensverwerking en de mate van zeggenschap waarmee de verwerking van persoonsgegevens gepaard gaat.²⁶⁵

²⁶⁵ Kamerstukken II 1997/98, 25 892, nr. 3, p. 99.

De verantwoordelijke die persoonsgegevens te zijner behoefte buiten zijn rechtstreeks gezag verwerkt wil hebben is op grond van artikel 14, tweede lid, van de Wbp verplicht een bewerkersovereenkomst te sluiten. De verplichtingen moeten over en weer duidelijk zijn neergelegd. Op de verantwoordelijke rust een zorgplicht daarvoor zorg te dragen. Niet alleen dient hij civielrechtelijk de bewerker voldoende te hebben duidelijk gemaakt hoe met de persoonsgegevens wordt omgegaan, tevens dient hij toe te zien op de feitelijke naleving van de aldus gecreëerde verplichtingen. Het moet gaan om juridisch bindende voorschriften.²⁶⁶

De overeenkomst tussen de verantwoordelijke en de bewerker moet naar haar aard betrekking hebben op de gegevensverwerking. Het contract mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is.²⁶⁷

Het kan niet gaan om mondelinge afspraken. De ratio is dat de betrokkene in geval jegens hem onrechtmatig wordt gehandeld, over de nodige bewijsstukken kan beschikken wanneer deze overeenkomstig de regels van het procesrecht een rol gaan spelen.²⁶⁸

Beoordeling

[VERTROUWELIJK: B] levert een encryptiesleutel op de [VERTROUWELIJK: apparatuur]. [VERTROUWELIJK].

Er wordt onderhoud en technische ondersteuning voor de [VERTROUWELIJK: apparatuur] geleverd door [VERTROUWELIJK: A]. Het CBP heeft vastgesteld dat [VERTROUWELIJK] (dan) toegang kunnen verkrijgen tot de statistische gegevens (inclusief versleutelde [VERTROUWELIJK: identifiers]).

[VERTROUWELIJK: B] en [VERTROUWELIJK: A] zijn niet aan het rechtstreeks gezag van Tele2 onderworpen.

Volgens Tele2 kunnen [[VERTROUWELIJK: B] en [VERTROUWELIJK: A] niet worden aangemerkt als bewerker, noch ten behoeve van Tele2 [VERTROUWELIJK], noch ten behoeve van Tele2 [VERTROUWELIJK], omdat [VERTROUWELIJK: B] en [VERTROUWELIJK: A] geen persoonsgegevens verwerken van klanten van Tele2 [VERTROUWELIJK].²⁶⁹

Door [VERTROUWELIJK], verwerkt [VERTROUWELIJK: B] gegevens. Omdat [VERTROUWELIJK: B] en [VERTROUWELIJK: A][VERTROUWELIJK] in staat zijn, al dan niet in opdracht van Tele2 [VERTROUWELIJK] en/of [VERTROUWELIJK: A], (om hen in staat te stellen) te allen tijde de [VERTROUWELIJK: identifiers] te (kunnen) ontsleutelen, is sprake van een verwerking van persoonsgegevens en dient Tele2 een bewerkersovereenkomst te sluiten met [VERTROUWELIJK: B] en [VERTROUWELIJK: A].

²⁶⁶ Idem.

²⁶⁷ Idem.

²⁶⁸ Idem, p. 102.

²⁶⁹ Zienswijze 1 Tele2, randnummers 66 en 67. Zie **bijlage III** bij dit rapport.

Het CBP heeft in paragraaf 2.4, onder het kopje 'Ondersteuning en onderhoud door [VERTROUWELIJK: A]' (p. 24 e.v. van dit rapport) vastgesteld dat Tele2 geen (bewerkers)overeenkomsten heeft gesloten met [VERTROUWELIJK: B] en [VERTROUWELIJK: A].²⁷⁰

Tele2 handelt in strijd met artikel 14 van de Wbp doordat zij geen bewerkersovereenkomst heeft gesloten met haar bewerkers [VERTROUWELIJK: B] en [VERTROUWELIJK: A].

Voorgestelde maatregel

Zoals beschreven in paragraaf 2.4, onder het kopje 'Voorgestelde maatregelen' (p. 25 e.v. van dit rapport) heeft Tele2 bij haar zienswijze 2 een concept bewerkersovereenkomst tussen [VERTROUWELIJK] ("Data Processor") en [VERTROUWELIJK] aan het CBP overgelegd die Tele2 bereid is overeen te komen, hoewel zij haar eerdere standpunt handhaaft dat noch [VERTROUWELIJK: B] noch [VERTROUWELIJK: A] kunnen worden aangemerkt als bewerkers in de zin van de Wbp.²⁷¹

De concept bewerkersovereenkomst bevat een verplichting voor [VERTROUWELIJK: B] om de persoonsgegevens slechts in opdracht van Tele2 te verwerken [VERTROUWELIJK]. De concept bewerkersovereenkomst bevat verder een verplichting voor [VERTROUWELIJK: B] om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, volgens het recht van [VERTROUWELIJK]. De concept bewerkersovereenkomst bevat ten slotte een bepaling dat [VERTROUWELIJK: B] gehoor zal geven aan een redelijk verzoek van Tele2 om te verifiëren of zij handelt in overeenstemming met haar verplichtingen als bewerk:

De overgelegde concept bewerkersovereenkomst bevat ten aanzien van [VERTROUWELIJK: B] niet de categorieën van verwerkte persoonsgegevens, de doeleinden (de opdracht aan de verwerker/verwerkingshandelingen) en afspraken over het al dan niet toestaan van verwerking door subbewerkers.²⁷²

De concept bewerkersovereenkomst bevat ten aanzien van [VERTROUWELIJK: A] onder andere de bepaling dat Tele2 en [VERTROUWELIJK: A] zich zullen houden aan de overgelegde concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] (data exporter) en [VERTROUWELIJK: A] (data importer) (toegevoegd Annex 1 bij de concept bewerkersovereenkomst). De concept doorgifte-overeenkomst bevat

²⁷⁰ Zie o.a. reactie Tele2 op rappel verzoek om inlichtingen van 2 december 2011, p. 2. De overeenkomsten tussen [VERTROUWELIJK] bevatten geen nadere contractuele verplichtingen ten aanzien van de beveiliging en geheimhouding van (vertrouwelijke informatie over) (de locatie van) de encryptiesleutel, zoals toegangsrechten, auditing en logging (en monitoring daarvan).

²⁷¹ Overeenkomst Tele2 [VERTROUWELIJK].

²⁷² Zienswijze 2 Tele2, randnummer 65. Zie **bijlage IV** bij dit rapport.

²⁷² WP29 169. Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker" van 16 februari 2010, p. 30, Kamerstukken II 1997/98, 25 892, nr. 3, p. 99 en CBP Richtsnoeren: Beveiliging van persoonsgegevens, *Scrt.* 2013, nr. 5174, p. 26.

verplichtingen voor [VERTROUWELIJK: A] om de persoonsgegevens slechts in opdracht van Tele2 te verwerken en passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (volgens het recht van [VERTROUWELIJK]), afspraken over toezicht op de naleving van de afspraken in de bewerkersovereenkomst, de categorieën van verwerkte persoonsgegevens, de doeleinden (activities relevant to the transfer en processing operations) en afspraken over het al dan niet toestaan van verwerking door subbewerkers.

Door het aangaan van de overgelegde concept bewerkersovereenkomst zal de geconstateerde overtreding van artikel 14 van de Wbp (bewerkersovereenkomst) worden beëindigd voor wat betreft de relatie met haar bewerker [VERTROUWELIJK: A]. Dit omdat de concept bewerkersovereenkomst met Annex de afspraken bevat die op grond van de wet zijn vereist. Voor wat betreft de relatie met haar bewerker [VERTROUWELIJK: B] zal door het aangaan van de overgelegde concept bewerkersovereenkomst de geconstateerde overtreding van artikel 14 van de Wbp worden beëindigd indien en voor zover de concept bewerkersovereenkomst wordt aangevuld met de categorieën van verwerkte persoonsgegevens, de doeleinden (de opdracht aan [VERTROUWELIJK: B]/verwerkings handelingen) en afspraken over het al dan niet toestaan van verwerking door subbewerkers.

3.11 Doorgifte

Uitwerking van het wettelijk kader

Op grond van artikel 76 van de Wbp mogen persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt slechts naar een land buiten de Europese Unie/Europese Economische Ruimte (EER) worden doorgegeven indien dat land een passend beschermingsniveau waarborgt.

Het passend karakter van het beschermingsniveau wordt beoordeeld gelet op de omstandigheden die op de doorgifte van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd (artikel 76, tweede lid, van de Wbp).

Artikel 77 van de Wbp bevat een aantal uitzonderingen op het hierboven genoemde doorgifteverbod. In dit geval komen alleen de uitzonderingsgronden, zoals genoemd in artikel 77, eerste lid, onder a tot en met c, en tweede lid, van de Wbp mogelijksterwijs in aanmerking:

Wanneer een land buiten de Europese Unie geen passend beschermingsniveau biedt, kan doorgifte van persoonsgegevens toch plaatsvinden, indien:

a. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven;

b. de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, 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 doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst;
 (...)
 g. gebruik wordt gemaakt van een modelcontract als bedoeld in artikel 26, vierde lid, van de Privacyrichtlijn [artikellid geparafraseerd door het CBP om de leesbaarheid te bevorderen].
 2. In afwijking van het eerste lid, kan Onze Minister, gehoord het College, een vergunning geven voor een doorgifte of een categorie van doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Aan de vergunning worden de nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.

Artikel 76 en verder van de Wbp stelt bijzondere eisen wanneer sprake is van vormen van gegevensverwerking die leiden tot de doorgifte van persoonsgegevens aan landen buiten de Europese Unie.

Met het begrip ‘doorgifte’ in dit artikel wordt bedoeld op het ter kennis brengen van de gegevens aan een persoon die zich bevindt buiten de rechtsmacht van één van de landen van de Europese Unie. Daaronder wordt ook verstaan het bieden van toegang tot de persoonsgegevens in landen buiten de Europese Unie zonder passend beschermingsniveau.²⁷³

Het uitgangspunt is dat de doorgifte van persoonsgegevens naar een land buiten de Europese Unie slechts mogelijk is indien dat andere land voldoende bescherming biedt, tenzij een van de uitzonderingen als genoemd in artikel 77 van de Wbp van toepassing is. Artikel 76, tweede lid, van de Wbp noemt een aantal criteria die bij de beoordeling in ieder geval in aanmerking moeten worden genomen.

Beoordeling

Het CBP heeft in paragraaf 2.4, onder het kopje 'Ondersteuning en onderhoud door [VERTROUWELIJK: A]' (zie p. 24 e.v. van dit rapport) vastgesteld dat Tele2 toegang biedt tot de persoonsgegevens aan [VERTROUWELIJK] in geval van onderhoud en/of storing.²⁷⁴ Er is in zoverre sprake van doorgifte.

[VERTROUWELIJK] zijn niet aangewezen door de Europese Commissie als landen met een passend beschermingsniveau, (mede) gelet op de algemene en sectoriële rechtsregels die in het betrokken derde land gelden. [VERTROUWELIJK] waarborgen geen passend beschermingsniveau. [VERTROUWELIJK].

²⁷³ Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP, p. 7. URL:

http://www.cbpweb.nl/downloads_int/Nota_derde_landen_nl.pdf (URL laatst bezocht op 29 mei 2013). Zie ook URL: http://www.cbpweb.nl/Pages/th_doo_watis.aspx (URL laatst bezocht op 29 mei 2013).

²⁷⁴ Reactie Tele2 op rappel verzoek om inlichtingen van 23 november 2011, p. 2.

Tele2 heeft geen doorgifteovereenkomst met [VERTROUWELIJK: A] gesloten om, rekening houdend met de aard van de persoonsgegevens, een passend beschermingsniveau te garanderen.

Tele2 heeft niet verklaard en uit het onderzoek is ook overigens niet gebleken dat Tele2 een beroep kan doen op de uitzonderingsgronden, zoals genoemd in artikel 77, eerste lid, onder a tot en met f, van de Wbp.

Tele2 heeft ter zake van de gegevensverwerkingen geen doorgiftevergunning verkregen als bedoeld in artikel 77, tweede lid, van de Wbp.

In haar zienswijzen betwist Tele2 dat sprake is van doorgifte, omdat medewerkers van [VERTROUWELIJK: A] die van buiten de EU onderhoud en ondersteuning bieden, geen toegang hebben tot persoonsgegevens van Tele2 [VERTROUWELIJK].²⁷⁵ De relevante toets is of toegang wordt geboden tot de persoonsgegevens in landen buiten de Europese Unie zonder passend beschermingsniveau.²⁷⁶ Het CBP heeft in paragraaf 3.3 (zie p. 34 e.v. van dit rapport) vastgesteld dat sprake is van de verwerking van persoonsgegevens en dat [VERTROUWELIJK: A] die van buiten de EU onderhoud en ondersteuning bieden, toegang kunnen hebben tot de persoonsgegevens van Tele2, al dan niet met medewerking van [VERTROUWELIJK] Tele2 of [VERTROUWELIJK: B].

Doordat Tele2 persoonsgegevens doorgeeft naar (dat wil zeggen: toegang tot de gegevens biedt in) landen buiten de Europese Unie zonder passend beschermingsniveau (te weten: [VERTROUWELIJK]) handelt zij in strijd met artikel 76 van de Wbp.

Voorgestelde maatregelen

In reactie op het Conceptrapport definitieve bevindingen heeft Tele2 een concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A] aan het CBP overgelegd die Tele2 voornemens is overeen te komen met [VERTROUWELIJK: A] zodra zij duidelijkheid heeft van het CBP dat de thans door Tele2 toegepaste hashing-oplossing, al dan niet met de voorgestelde additionele maatregelen, in de toekomst kan worden voortgezet.²⁷⁷

Tele2 gebruikt voor de concept doorgifte-overeenkomst het door de Europese Commissie goedgekeurde modelcontract voor doorgifte naar een bewerker in een derde land (Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under

²⁷⁵ Zienswijze 1 Tele2, randnummer 72. Zie **bijlage III** bij dit rapport.

²⁷⁶ Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP, p. 7. URL: http://www.cbpweb.nl/downloads_int/Nota_derde_landen_nl.pdf (URL laatst bezocht op 29 mei 2013). Zie ook URL: http://www.cbpweb.nl/Pages/th_doo_watis.aspx (URL laatst bezocht op 29 mei 2013).

²⁷⁷ Zienswijze 2 Tele2, randnummer 67. Zie **bijlage IV** bij dit rapport.

document C(2010) 593)).²⁷⁸ De bepalingen van het modelcontract zijn ongewijzigd overgenomen. Appendix 2 bij de concept doorgifte-overeenkomst/het modelcontract (Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached)) is thans nog niet ingevuld:[VERTROUWELIJK].

Door gebruik te maken van, oftewel het aangaan van een volledig ingevuld en ongewijzigd modelcontract voor doorgifte naar een bewerker in een derde land, zoals een door [VERTROUWELIJK] partijen getekende versie van de overgelegde concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A], aangevuld met een ingevulde Appendix 2, zal de geconstateerde overtreding van artikel 76 van de Wbp (doorgifte) worden beëindigd. Door hier gebruik van te maken zal Tele2 een beroep toekomen op een uitzondering op het doorgifteverbod.

4. CONCLUSIE

Tele2 past data-analyse technieken toe op het dataverkeer in haar mobiele netwerk. Naar schatting 250.000 Tele2 abonnees met een (prepaid of postpaid) data abonnement maken gebruik van dataverkeersdiensten van Tele2.

Tele2 verwerkt gegevens over en uit het dataverkeer van deze abonnees. Deze gegevens betreffen een [VERTROUWELIJK: identifier] in combinatie met gegevens over het bezoek aan en gebruik van apps, websites en protocollen.

Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn. De persoonsgegevens worden door Tele2 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 Tele2 direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon, omdat Tele2 een koppeling(smogelijkheid) heeft met het [VERTROUWELIJK: identifier], NAW-gegevens en/of (een) e-mailadres(sen).

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 toestelidentifiers (bijvoorbeeld het telefoonnummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume, hostnames, etc.)
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk spam-, virus- en malwareherkenningsgegevens uit de inhoud van het e-mailverkeer

Tele2 verwerkt de persoonsgegevens voor de doeleinden van netwerkbeheer en marktonderzoek en ten behoeve van spam, virus- en spywarebestrijding in het e-mailverkeer.

²⁷⁸ URL: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (URL laatst bezocht op 29 mei 2013).

Geconstateerde overtredingen

De Wbp stelt eisen aan het verwerken van persoonsgegevens. Eén van die eisen is dat er een rechtvaardigingsgrond (grondslag) moet zijn voor de verwerking. Het CBP heeft bij Tele2 een aantal overtredingen van de Wbp en de Tw geconstateerd.

Netwerkbeheer en marktonderzoek

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

Hoewel Tele2 [VERTROUWELIJK: identifier] versleutelt en andere identificerende gegevens alleen gedurende de internetssessie van een abonnee vastlegt, leidt de toegepaste versleuteling niet tot onomkeerbare anonimisering. De verzamelde gegevens blijven daardoor persoonsgegevens. Omdat de huidige werkwijze van Tele2 voor het doeleinde van netwerkbeheer niet voldoet aan de vereisten van proportionaliteit en subsidiariteit, is van een noodzaak voor het gebruiken, vastleggen en bewaren van persoonsgegevens geen sprake. Omdat Tele2 ook geen ander noodzakelijk verwerkingsdoeleinde heeft voor deze gegevensverwerking, handelt Tele2 in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Verder mogen deze gegevens niet zonder ondubbelzinnige toestemming van de abonnees worden verwerkt voor marktonderzoek. Omdat Tele2 de (versleutelde) gegevens voor marktonderzoeksdoeleinden gebruikt, en deze ondubbelzinnige toestemming niet heeft verkregen, handelt Tele2 in strijd met (artikel 11.5 van de Tw jo.) artikel 7 en 8 van de Wbp.

Meldingsplicht

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen wettelijk verplicht deze gegevensverwerking te melden bij het CBP. De meldingen van Tele2 bevatten echter geen, of onvoldoende duidelijke informatie over de doeleinden waarvoor Tele2 persoonsgegevens verwerkt. Tele2 handelt hierdoor in strijd met artikel 7 jo. 27 en 28 van de Wbp.

Uitdrukkelijk omschreven en gerechtvaardigde doeleinden

Doordat Tele2 de doeleinden netwerkbeheer en marktonderzoek, spam- virus en spywarefiltering van het e-mailverkeer evenals prepaidverkeer waarvoor zij persoonsgegevens verwerkt(e) onvolledig en onvoldoende duidelijk heeft omschreven bij de meldingen die zij bij het CBP heeft gedaan, worden de door Tele2 verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelt Tele2 daarmee ook in strijd met artikel 7 van de Wbp.

Doordat de gegevensverwerking voor de doeleinden netwerkbeheer en marktonderzoek niet in alle stadia kan steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, worden de door Tele2 verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelt Tele2 daarmee ook in strijd met artikel 7 van de Wbp.

Informeren abonnees

Tele2 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. Tele2 informeerde abonnees (tot april 2013) onvoldoende over de soorten persoonsgegevens die zij met de toepassing van data-analysetechnieken verkrijgt voor het doeleinde netwerkbeheer en marktonderzoek. Daarnaast informeerde Tele2 hen niet over de soorten verkeersgegevens, de doeleinden van de verwerking en de bewaartermijn. Tele2 handelde hierdoor (en handelt ten dele nog steeds) in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

Bewerkersovereenkomst

Op grond van de Wbp is een bedrijf verplicht een bewerkersovereenkomst te sluiten als een ander ten behoeve van het bedrijf persoonsgegevens verwerkt. [VERTROUWELIJK: B/A] levert onderhoud en technische ondersteuning op de data-analyse apparatuur. Tele2 handelt in strijd met artikel 14 van de Wbp doordat zij geen bewerkersovereenkomsten heeft gesloten met haar bewerker(s) [VERTROUWELIJK: B/A].

Internationale gegevensverstrekking

Doorgifte van persoonsgegevens naar een land buiten de Europese Unie is alleen toegestaan als dit land een passend beschermingsniveau biedt. In geval van onderhoud en/of storing biedt Tele2 toegang tot de persoonsgegevens aan [VERTROUWELIJK: A] in twee landen die dit niveau niet bieden: [VERTROUWELIJK]. Tele2 handelt hierdoor in strijd met artikel 76 van de Wbp.

Geen overtredingen

Spam- en virusfiltering e-mailverkeer

Tele2 heeft een wettelijke grondslag voor de gegevensverwerking ten behoeve van spam-, virus- en spywarefiltering van het e-mailverkeer. Op dit punt is Tele2 dan ook niet in overtreding (geweest).

Prepaidverkeer

Tot april 2012 verwerkte Tele2 persoonsgegevens om het bezoek aan en gebruik van (gratis) opwaardeersites te faciliteren van prepaid-abonnees bij een ontoereikend tegoed. Omdat Tele2 hierbij [VERTROUWELIJK], en geen gegevens over deze data-analyse bewaarde, was de werkwijze proportioneel. Tele2 was hierdoor niet in overtreding.

Getroffen maatregelen

Naar aanleiding van het onderzoek heeft Tele2 in april 2013 een (algemeen) Privacy Statement gepubliceerd. Door deze maatregel zijn de geconstateerde overtredingen met betrekking tot de informatieplicht gedeeltelijk beëindigd. De geconstateerde overtredingen van artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp duren (wel) verder voort op het gebied van het ontbreken van informatie aan abonnees over de duur van de verwerking (bewaartermijnen) en het doeleinde van de verwerking voor marktonderzoek.

Voorgestelde maatregelen

Tele2 heeft twee alternatieve wijzigingen voorgesteld van de wijze van versleuteling van de [VERTROUWELIJK: identifieer]. Toepassing van deze methodes leidt echter niet tot de conclusie dat geen sprake meer is van persoonsgegevens. Invoering ervan leidt dan ook niet tot beëindiging van de geconstateerde overtredingen.

Tele2 heeft concept wijzigingen en aanvullingen gestuurd op de melding bij het CBP en een beknopte tekst voor een privacy verklaring. Deze maatregelen leiden echter, ook na daadwerkelijke invoering ervan, (nog) niet tot beëindiging van de geconstateerde overtredingen van de artikelen 34 en 27 jo. 28 van de Wbp.

Tele2 heeft tevens [VERTROUWELIJK] conceptovereenkomsten toegestuurd om de geconstateerde overtredingen te beëindigen ten aanzien van (het inschakelen van) bewerkers en internationale doorgifte van persoonsgegevens.

Door het aangaan van de overgelegde concept bewerkersovereenkomst zal de geconstateerde overtreding van artikel 14 van de Wbp (bewerkersovereenkomst) worden beëindigd voor wat betreft de relatie met haar bewerkster [VERTROUWELIJK: A].

Voor wat betreft de relatie met haar bewerkster [VERTROUWELIJK: B] zal door het aangaan van de overgelegde concept bewerkersovereenkomst de geconstateerde overtreding van artikel 14 van de Wbp worden beëindigd indien en voor zover de concept bewerkersovereenkomst wordt aangevuld met de categorieën van verwerkte persoonsgegevens, de doeleinden (de opdracht aan [VERTROUWELIJK: B]/verwerkings handelingen) en afspraken over het al dan niet toestaan van verwerking door subbewerker.

Door gebruik te maken van een door [VERTROUWELIJK] partijen getekende versie van de overgelegde concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A], aangevuld met een ingevulde Appendix 2, zal de geconstateerde overtreding van artikel 76 van de Wbp (doorgifte) worden beëindigd.

Bijlage I Overzicht mobiel netwerk Tele2²⁷⁹

[VERTROUWELIJK]

²⁷⁹ Bijlage 1 bij reactie Tele2 op verzoek om inlichtingen van 19 september 2011.
OPENBARE VERSIE Rapport definitieve bevindingen van 29 mei 2013

Bijlage II Verklarende woordenlijst

APN (Access Point Name)	Naam van het externe netwerk waarmee de GGSN verbinding legt, zoals het internet of bijvoorbeeld de MMS-server.
Core netwerk	Het core netwerk van een mobiele operator verzorgt het afwickelen van telefonie- en dataverkeer vanaf het netwerk van zendmasten. Het core netwerk stelt mobieltjes in staat om onderling met elkaar te communiceren en met mobieltjes van andere (wereldwijde) operators.
Fair Use Policy	Term die door operators en providers wordt gebruikt om 'normaal datagebruik' te omschrijven, in tegenstelling tot abonnementen met een vaste hoeveelheid toegestaan dataverkeer per maand.
GGSN (<i>Gateway GPRS Support Node</i>)	Netwerkapparatuur die de signaleringen en het dataverkeer doorgeeft aan externe netwerken, zoals het internet.
GPRS (<i>General Packet Radio Service</i>)	Standaard voor het afwickelen van mobiel dataverkeer.
GSM (<i>Global System for Mobile Communications</i>)	Standaard voor het afwickelen van mobiel spraakverkeer. Sinds midden jaren negentig kan via GSM ook dataverkeer worden afgewikkeld. Dat wordt ook wel 2G-verkeer genoemd, <i>Second Generation Wireless Digital Technology</i> .
Hash	Wiskundige berekening die grotere dataverzamelingen van verschillende omvang kan omzetten naar kleinere dataverzamelingen met een vaste lengte.
HLR (<i>Home Location Register</i>)	Database met eigenschappen van het mobiele abonnement: prepaid of abonnement, wel of niet mogen bellen in het buitenland (roaming), doorschakelingen, blokkades, enz. De HLR houdt ook de geografische positie van het toestel bij (via zendmastgegevens uit het VLR).
IMEI (<i>International Mobile Equipment Identity</i>)	Wereldwijd uniek 15-cijferig nummer in de hardware van smartphones, waarmee ook de fabrikant van het besturingssysteem kan worden herkend, zoals Blackberry (RIM), Android (Google) of iOS (Apple).

IMSI (<i>International Mobile Subscriber Identity</i>)	Voor klanten van mobiele telefonie 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 (<i>Mobile Subscriber Integrated Services Digital Network-Number</i>)	Wereldwijd uniek telefoonnummer. Een MSISDN bestaat uit maximaal 15 posities, beginnend met de landcode, gevolgd door een netnummer en de tien nummers van het eigenlijke telefoonnummer (in Nederland: 06-nummer).
MVNO (<i>Mobile Virtual Network Operator</i>)	Een (MVNO) is een bedrijf dat niet over een licentie beschikt, maar onder eigen merknaam mobiele telefonie verkoopt over het netwerk van een andere mobiele operator.
Radiotoegangsnetwerk	Het radiotoegangsnetwerk van een mobiele operator verzorgt het afwickelen 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 (<i>Serving GPRS Support Node</i>)	Netwerkapparatuur die mobiel data- en signaleringsverkeer afwikkelt van en naar zendmasten in het (eigen) netwerk. De SGSN houdt tevens locatiegegevens bij op zendmastniveau, en speelt een kernrol bij de authenticatie van abonnees en het factureren.
Signalering	Kleine berichten die nodig zijn om de verbinding op te bouwen, in stand te houden en te verbreken.
UMTS (<i>Universal Mobile Telecommunications Service</i>)	Standaard voor het afwickelen van breedband mobiel dataverkeer, ook wel 3G genaamd. UMTS is de opvolger van GPRS als standaardtechnologie om

	mobiel dataverkeer af te wikkelen.
VLR (<i>Visitor Location Register</i>)	Database met de exacte locaties van alle abonnees in het eigen service-gebied van de operator. Deze informatie is noodzakelijk om gesprekken af te leveren bij de juiste zendmast.

Bijlage III Zienswijze 1 van Tele2 op de Voorlopige Bevindingen, met de reactie daarop van het CBP (zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd én aangevuld in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van het Conceptrapport definitieve bevindingen).

Opmerkingen en aanvullingen feitelijk kader

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat zij inmiddels een compliance-officer heeft aangesteld, die zich mede zal richten op de naleving van de privacy-regelgeving.²⁸⁰

Reactie CBP: Het CBP heeft dit gegeven opgenomen in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Zienswijze 1 Tele2: In haar zienswijze schrijft Tele2 dat de netwerkbelasting die smartphones en apps veroorzaken niet op andere manieren kan worden gemeten. *"Aan algemene marktmonitors en klantenpanels kan Tele2 geen nauwkeurige, statistische informatie ontlelen over welk gebruik klanten daadwerkelijk maken van het mobiele netwerk."*²⁸¹

Reactie CBP: Het CBP heeft deze zienswijze toegevoegd aan de feitelijke bevindingen in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport, omdat het geen aanpassing vergt van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat er een proportioneel alternatief is voor de door Tele2 ingezette data-analysetool waardoor de verkeersgegevens direct onomkeerbaar worden geanonimiseerd.

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat het CBP zich - ten onrechte - lijkt te baseren op (algemene) technische documentatie (handleidingen of contractuele documentatie), zonder dat bij Tele2 geverifieerd is of de feitelijke implementatie van de technologie ten behoeve van Tele2 daarmee overeenstemt.²⁸²

Reactie CBP: Bevindingen in hoofdstukken 2 en 3 van het Rapport voorlopige bevindingen zijn gebaseerd op de feitelijke instellingen van de gebruikte data-analyse apparatuur, zoals afgeleid uit de antwoorden van Tele2 op de inlichtingenverzoeken van het CBP en OPTA (die zijn gecontroleerd aan de hand van de bijbehorende (product)documentatie). De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Zienswijze 1 Tele2: In haar zienswijze geeft Tele2 aan dat de [VERTROUWELIJK: apparatuur]-technologie alleen screent op vooraf gedefinieerde signatures (domeinen). [VERTROUWELIJK].²⁸³

²⁸⁰ Zienswijze 1 Tele2 van 29 februari 2012, randnummer 19.

²⁸¹ Idem, randnummer 64.

²⁸² Idem, randnummer 26.

²⁸³ Idem, randnummers 31 en 32.

Reactie CBP: De zienswijze 1 van Tele2 heeft op het punt van (de werkwijze van Tele2 bij) de inzet van data-analysetechnieken geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport, omdat het geen aanpassing vergt van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat Tele2 inhoudelijke communicatiegegevens verwerkt, niet alleen met betrekking tot http-verkeer, maar ook met betrekking tot (gebruik van) apps.

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat het rapport ten onrechte melding maakt van vastlegging van [VERTROUWELIJK: identifiers].²⁸⁴

Reactie CBP: Het CBP heeft deze feiten gecorrigeerd in het Conceptrapport definitieve bevindingen. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport, omdat het geen aanpassing vergt van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat Tele2 (via de VERTROUWELIJK: identifiers) persoonsgegevens verzamelt en verwerkt.

Persoonsgegevens

Zienswijze 1 Tele2: Tele2 geeft aan dat de NAW-gegevens van veel prepaid abonnees onbekend zijn.²⁸⁵

Reactie CBP: Ten aanzien van de prepaid abonnees van wie Tele2 geen NAW-gegevens en/of e-mailadressen heeft, beschikt Tele2 wel over ten minste [VERTROUWELIJK: identifier], en gedurende een datasessie, ook over [VERTROUWELIJK: identifiers].

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 geregistreeerde 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).*²⁸⁶

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

²⁸⁴ Idem, randnummer 40.

²⁸⁵ Idem, randnummer 43.

²⁸⁶ WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 14-15.

“(...) 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.”²⁸⁷

De zienswijze 1 van Tele2 heeft op het punt van de identificeerbaarheid van de prepaid abonnees geleid tot aanvulling van de feitelijke bevindingen en beoordeling in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Hashing

Zienswijze 1 Tele2: Tele2 schrijft in haar zienswijze dat [VERTROUWELIJK].²⁸⁸

Tele2 verklaart in dat verband: [VERTROUWELIJK].²⁸⁹

[VERTROUWELIJK]

Reactie CBP: De zienswijze 1 van Tele2 heeft op het punt van de werkwijze met betrekking tot hashing geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport, omdat het geen aanpassing vergt van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat de gehashte [VERTROUWELIJK: identifiers] herleidbaar zijn tot individuen, door Tele2 of door [VERTROUWELIJK: A/B].

Zienswijze 1 Tele2: Tele2 schrijft in haar zienswijze [VERTROUWELIJK].²⁹⁰

Reactie CBP: Wat er verder ook zij van de [VERTROUWELIJK] beveiligingsmaatregelen en de expertise van (de medewerkers van) Tele2, het CBP heeft in het rapport vastgesteld dat er ook andere manieren zijn om de verwerkte gegevens te herleiden tot een individuele natuurlijke persoon, bijvoorbeeld (her)identificatie zonder de naam van de abonnee door Tele2 [VERTROUWELIJK] dan wel ontsleuteling door Tele2 [VERTROUWELIJK] (via [VERTROUWELIJK: B] en/of [VERTROUWELIJK: A]), en [VERTROUWELIJK: B] en/of [VERTROUWELIJK: A]. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport, omdat het geen aanpassing vergt van dragende of doorslaggevende argumenten ter onderbouwing van het oordeel dat de gehashte [VERTROUWELIJK: identifiers] herleidbaar zijn tot individuen, door Tele2 of door [VERTROUWELIJK: A/B].

Bewerkersovereenkomst en doorgifte

Zienswijze 1 Tele2: Tele2 schrijft in haar zienswijze: [VERTROUWELIJK].²⁹¹

²⁸⁷ HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

²⁸⁸ Zienswijze 1 Tele2, randnummer 46.

²⁸⁹ Reactie Tele2 op verzoek om inlichtingen van 9 november 2011, p. 2.

²⁹⁰ Idem, randnummer 48.

²⁹¹ Idem, randnummer 67.

Tele2 licht in haar zienswijze nader toe dat [VERTROUWELIJK].²⁹²

Reactie CBP: Het CBP leidt hieruit af dat Tele2 hiermee wil zeggen dat onderhoud en technische ondersteuning voor de [VERTROUWELIJK: apparatuur] wordt geleverd door [VERTROUWELIJK: A] en niet door [VERTROUWELIJK: B]. Op dit punt zijn de feitelijke bevindingen in het rapport aangevuld.

Zienswijze 1 Tele2: Tele2 stelt dat een bewerkersovereenkomst niet is vereist, omdat [VERTROUWELIJK: A/B] niet kan *"worden aangemerkt als een bewerker in de zin van de Wbp, noch ten behoeve van Tele2 [VERTROUWELIJK]. [VERTROUWELIJK: A/B] heeft slechts bepaalde technologie verkocht en geleverd aan Tele2 [VERTROUWELIJK].* Tele2 geeft aan dat het haar voorkeur heeft om te komen tot een zodanig niveau van encryptie van de [VERTROUWELIJK: identifiërs] dat ook volgens het CBP niet langer sprake is van persoonsgegevens. Mocht dat echter niet haalbaar blijken, dan is Tele2 bereid om met [VERTROUWELIJK: A/B] in overleg te treden over het aangaan van een bewerkers- en doorgifteovereenkomst.²⁹³

Reactie CBP: De bereidheid van Tele2 om een bewerkers- en doorgifteovereenkomst te sluiten met [VERTROUWELIJK: A/B] is als gegeven toegevoegd aan de feitelijke bevindingen in het rapport.

Omdat het een voornemen van Tele2 betreft, geen getroffen maatregel, heeft de zienswijze 1 van Tele2 op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Samenloop Wbp/Tw

Zienswijze 1 Tele2: Tele2 betoogt dat de data-analyse in belangrijke mate betrekking heeft op verkeersgegevens in de zin van hoofdstuk 11 van de Tw. Als al aan de toepassing van de Wbp wordt toegekomen, brengt de samenloop met de Tw volgens Tele2 mee dat bij de invulling van de normen van de Wbp in elk geval niet voorbij mag worden gegaan aan de specifieke invulling die daaraan door de (Nederlandse en Europese) wetgever is gegeven voor de telecommunicatiesector.²⁹⁴ Tele2 benadrukt dat netwerkbeheer onder de e-Privacyrichtlijn uitdrukkelijk is erkend als legitiem doel voor de tijdelijke opslag van communicatie- en verkeersgegevens, mits het vertrouwelijke karakter gewaarborgd blijft.²⁹⁵

Reactie CBP: Het CBP heeft in reactie hierop in het Conceptrapport definitieve bevindingen, vastgesteld dat de persoonsgegevens kunnen worden ingedeeld in twee categorieën:

1. persoonsgegevens die tevens communicatie zijn (en dus geen verkeersgegevens), namelijk gegevens zoals hostnames (URL op hoofddomein), referers (laatst bezochte URL) en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer

²⁹² Idem, randnummer 46.

²⁹³ Idem, randnummers 70 en 73.

²⁹⁴ Idem, randnummer 23

²⁹⁵ Idem, randnummer 59.

2. persoonsgegevens die tevens verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestelidentifiers, de starttijd en eindtijd van de data sessie, verbruikte datavolume etc.

Elke categorie van persoonsgegevens heeft een eigen beoordelingskader.

Persoonsgegevens, tevens communicatie: hostnames, referers en spam-, virus- en malwareherkenningsgegevens

Ten aanzien van hostnames, referers en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer, geldt dat geen sprake is van verkeersgegevens, maar van communicatie (tevens persoonsgegevens).²⁹⁶ Artikel 8 van de Wbp is van toepassing, zij het dat (richtlijnconforme uitleg²⁹⁷ van) artikel 5, eerste lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw (nieuw)), voor zover voor dit onderzoek van belang, op dit punt een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen.

Persoonsgegevens, tevens verkeersgegevens: overige gegevens over het dataverkeer

Ten aanzien van de overige gegevens over het dataverkeer, geldt dat sprake is van persoonsgegevens, tevens verkeersgegevens. Artikel 8 van de Wbp is van toepassing, zij het dat artikel 11.5 van de Tw op dit punt een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp.

De zienswijze 1 van Tele2 heeft op het punt van de samenloop van Wbp en Tw, meer in het bijzonder de toetsing van de grondslag voor (i) de verwerking van persoonsgegevens die ook verkeersgegevens zijn en (ii) de verwerking van communicatie, tevens persoonsgegevens, geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat de door Tele2 ingezette data-analysetechnieken voor het doeleinde van netwerkbeheer niet proportioneel zijn.

Verkeersbeheer

Zienswijze 1 Tele2: Tele2 schrijft in haar zienswijze: [VERTROUWELIJK].²⁹⁸

Tele2 geeft in haar zienswijze aan dat als identificatie aan de hand van het versleutelde [VERTROUWELIJK: identifier] redelijkerwijs niet is uitgesloten *“dat de gekozen werkwijze in elk geval bijdraagt aan de legitimering van haar gebruik van deze informatie, en aan de beveiliging die zij ten aanzien van persoons- en verkeersgegevens in acht moet nemen. In dat verband wijst Tele2 [VERTROUWELIJK] erop dat zij op grond van de Wbp niet verplicht is om steeds de allerswaarste beveiliging te kiezen. Niettemin staat Tele2 [VERTROUWELIJK] open voor betere alternatieven voor de wijze van versleuteling dan wel anonimisatie.”*²⁹⁹ Tele2 voegt daaraan toe: Tele2 betoogt: *“(…) de Wbp [strekt,*

²⁹⁶ 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.

²⁹⁷ 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*).

²⁹⁸ Zienswijze 1 Tele2, randnummer 45.

²⁹⁹ Idem, randnummers 49 tot en met 51.

toevoeging door het CBP] er niet toe (...) dat een verantwoordelijke steeds de best beschikbare oplossing kiest. Met het feit dat er wellicht een - uit privacy-perspectief - betere oplossing bestaat, is dus niet gezegd dat het gebruik van alternatieven daarmee opeens strijdig is met de Wbp.”³⁰⁰ En: “Maar wellicht belangrijker is dat het volgens Tele2 [VERTROUWELIJK] mogelijk moet zijn de [VERTROUWELIJK: apparatuur]-technologie met relatief beperkte aanpassingen in lijn te brengen met de eisen die in het Rapport worden gesteld. (...) Binnen de [VERTROUWELIJK: apparatuur]-technologie worden [VERTROUWELIJK]. Het enige verschil met de aangehaalde eisen van het Rapport lijkt dus te zijn dat geen onomkeerbare versleuteling wordt toegepast.”³⁰¹

Reactie CBP: In het rapport worden voorbeelden gebruikt van technische alternatieven 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 door Tele2, althans geaggregeerd per abonnee niet ‘noodzakelijk’ en ‘in overeenstemming met het subsidiariteitsbeginsel’ is. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport dat de door Tele2 ingezette data-analysetechnieken voor het doeleinde van netwerkbeheer niet proportioneel zijn.

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat zij slechts terughoudend gebruik maakt van de [VERTROUWELIJK: apparatuur]-technologie, en de daardoor gegenereerde informatie thans uitsluitend gebruikt om aan de hand van algemene verkeersstatistieken het dataverkeer op het mobiele netwerk in goede banen te leiden, tijdig capaciteitsbeperkingen en congestie waar te nemen, en om haar netwerk adequaat te dimensioneren. Dit terwijl uit een recente opinie van de Europese Toezichthouder voor gegevensbescherming (EDPS) over netneutraliteit, netwerkbeheer en bescherming van persoonsgegevens zou blijken dat zelfs zulke, meer ingrijpende toepassingen in het kader van netwerkbeheer geoorloofd kunnen zijn (gedacht kan worden aan inzet van data-analyse technieken om video-streaming op een efficiëntere manier aan te bieden aan mobiele gebruikers). In het licht daarvan kan volgens Tele2 niet worden ingezien waarom de toepassing door Tele2 niet zou voldoen aan de eisen van proportionaliteit en subsidiariteit. Dit geldt temeer nu Tele2 verscheidene waarborgen heeft getroffen om het vertrouwelijke karakter van de communicatie te waarborgen, bijvoorbeeld het beperkte gebruik van de mogelijkheden die de [VERTROUWELIJK: apparatuur]-technologie in theorie biedt ([VERTROUWELIJK]) en versleuteling van de [VERTROUWELIJK: identifiers].³⁰²

Reactie CBP: In algemene zin geldt dat bij de toepassing van data-analyse technieken door mobiele aanbieders op het dataverkeer (inclusief signaleringsverkeer) van hun abonnees, gelet op de aard van de verzamelde persoonsgegevens en de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor gegevensvergaring in de vorm van data-analyse technieken naar aanleiding van het gebruik van het netwerk van de aanbieders), bovengemiddeld rekening moet worden gehouden met het risico (kans x impact) van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan

³⁰⁰ Idem, randnummer 58.

³⁰¹ Idem, randnummers 60 en 61.

³⁰² Idem.

waarvoor de gegevens oorspronkelijk zijn verzameld. Het herkennen/identificeren van het bezoek aan en gebruik van apps en websites kan leiden tot een omvangrijke verzameling van gevoelige persoonsgegevens die iets (kunnen) zeggen over het gedrag van mensen op internet. 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 en websites op zich niet ongevaarlijk. Ook hostnames (URL's 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 oneigenlijk gebruik van gegevens te voorkomen, (beveiligings)incidenten niet altijd kunnen worden voorkomen. Het hashen van het [VERTROUWELIJK: identifier] is een waarborg ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp. Gelet op de aard van de verzamelde persoonsgegevens en de potentiële waarde daarvan voor het bepalen van de toekomstige business strategie, bieden andere maatregelen dan het direct na het verzamelen verwijderen van de persoonsgegevens uit de verkregen dataset, bijvoorbeeld door onomkeerbare anonimisering in niet-persistent (werk)geheugen, onvoldoende waarborgen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de betrokken abonnees.

De opinie van de EDPS over netneutraliteit, netwerkbeheer en bescherming van persoonsgegevens noemt videocompressie overigens louter als voorbeeld van gebruikte data-analyse technieken, zonder oordeel: *"The reasons for ISPs to inspect and differentiate traffic are manifold. For example, traffic management policies may help ISPs to manage traffic during periods of high congestion, for example, by prioritising certain time-sensitive traffic, such as video streaming and downgrading other types of traffic which may be less time sensitive, such as P2P. The quality of real-time applications such as video streaming is, among other things, dependent on latency, i.e., delay due for example to network congestion."*³⁰³

De zienswijze 1 van Tele2 heeft op het punt van de noodzaak geleid tot aanvulling van de beoordeling in het rapport. De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

Marketingdoeleinden

Zienswijze 1 Tele2: Tele2 schrijft "dat er nooit sprake is geweest van marketingdoeleinden in de zin dat zij de gegevens gebruikte om op basis daarvan individuele aanbiedingen te doen.

³⁰³ Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, dated 7 October 2011, p. 3-4. URL: [http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_\(1\)_15_rt_2011.pdf](http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf) (URL laatst bezocht op 29 mei 2013).

*Zoals Tele2 [VERTROUWELIJK] aan het Cbp heeft aangegeven (in haar brief van 19 september 2011) is het wel zo dat de statistische informatie ook bedoeld was om in algemene zin het functioneren van de dienst en de prijs/kwaliteit verhouding daarvan te blijven optimaliseren. Dat ligt eerder in het verlengde van netwerkbeheer dan dat werkelijk sprake is van analyse van verkeersgegevens voor marketing of verkoopactiviteiten (in de zin van art. 6 van de e-Privacy richtlijn)."*³⁰⁴

Reactie CBP: De verklaring van Tele2 uit de brief van 19 september 2011 dat zij met marketingdoeleinden niet bedoelde het maken van individuele profielen of aanbiedingen was al opgenomen in het feitelijk kader in de voorlopige bevindingen.

De verwerking van niet-geanonimiseerde verkeersgegevens is toelaatbaar indien deze noodzakelijk is voor 'netwerkbeheer'. Het CBP beoordeelt deze noodzaak als volgt.

Het CBP heeft in het Conceptrapport definitieve bevindingen vastgesteld dat het verzamelen, gebruiken, vastleggen en bewaren van de persoonsgegevens door Tele2 over het bezoek aan en gebruik van apps en websites op individueel persoonsniveau, althans geaggregeerd per abonnee voor netwerkbeheer en (algemene) marketingdoeleinden zoals dat thans door Tele2 plaatsvindt, niet 'noodzakelijk' en 'proportioneel'/'in overeenstemming met het subsidiariteitsbeginsel' is.

Nu het verzamelen, gebruiken, vastleggen en bewaren van de verwerkte persoonsgegevens door Tele2 over het bezoek aan en gebruik van apps en websites op individueel persoonsniveau, althans geaggregeerd per abonnee niet noodzakelijk is voor de genoemde doeleinden³⁰⁵, en Tele2 ook geen andere grondslag heeft voor de in deze paragraaf 3.6.1 besproken verwerking van persoonsgegevens, handelt Tele2 in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

De zienswijze 1 van Tele2 heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport.

³⁰⁴ Zienswijze 1 Tele2, randnummer 63.

³⁰⁵ Vgl. ook overweging 29 van de e-Privacyrichtlijn: "De dienstenaanbieder mag zo nodig in individuele gevallen verkeersgegevens met betrekking tot abonnees en gebruikers verwerken om technische defecten of fouten in de transmissie van communicatie op te sporen. Verkeersgegevens die nodig zijn voor facturatie mogen ook door de aanbieder worden verwerkt om op het spoor te komen van en een einde te maken aan fraude in de vorm van het niet betalen voor het gebruik van de elektronische-communicatiedienst." Hieruit kan a contrario worden afgeleid dat voor het meer algemene doel van verkeersbeheer de verwerking slechts in geaggregeerde vorm is toegelaten. Het begrip 'geaggregeerde verkeersgegevens' omvat ingevolge overweging 30 van de e-Privacyrichtlijn "verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht." De verwerking zoals die thans door Tele2 plaatsvindt, kan niet worden aangemerkt als verwerking in geaggregeerde vorm. Het gaat om persoonsgegevens, tevens verkeersgegevens op individueel persoonsniveau, althans op persoonsniveau geaggregeerde gegevens: (technische) persoonsgegevens over het functioneren van het netwerk bij het gebruik daarvan door een individuele betrokkene. De verwerking van persoonsgegevens gaat verder dan de overbrenging van communicatie en de facturering ervan. De verwerking kan dan ook niet worden gebaseerd op de grondslag facturering, meer in het bijzonder het afgeleide doeleinde verkeersbeheer (artikel 11.5, tweede jo. vijfde lid, van de Tw jo. artikel 8 van de Wbp).

Getroffen maatregelen

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat zij heeft besloten om toepassing van de onderzochte data-analyse technieken (tijdelijk) op te schorten, uiterlijk met ingang van 11 april 2012, tenzij zij binnen die termijn andere maatregelen kan treffen om de door het CBP gesignaleerde bezwaren weg te nemen, zoals een verzwaring van de versleuteling en het vragen van ondubbelzinnige toestemming aan prepaid abonnees.³⁰⁶ Tele2 schrijft in haar zienswijze: [VERTROUWELIJK]. Tele2 geeft aan er vanuit te gaan dat met deze beslissing aan de overtredingen die de betreffende data-analyse technieken volgens het rapport voorlopige bevindingen veroorzaken hoe dan ook op afzienbare tijd een einde zal komen.³⁰⁷

Bij brief van 11 april 2012 heeft Tele2 het CBP laten weten dat nadere informatie over de gebruikte versleuteling bij de data-analyse apparatuur voor netwerkbeheer en marketingdoeleinden er volgens Tele2 toe leidt dat er geen sprake is van persoonsgegevens. Tele2 schrijft in haar brief van 11 april 2012: *"Tele2 is van mening dat de thans in de [VERTROUWELIJK: apparatuur] toegepaste encryptie reeds voldoende is om aan de verwerkte gegevens (of in elk geval het [VERTROUWELIJK: identifieer]) het identificerende karakter te ontnemen, en dat geen sprake is van persoonsgegevens. (...) Tele2 verzoekt het CBP zich over de toereikendheid van de toegepaste versleuteling uit te laten in haar definitieve rapport van bevindingen."*³⁰⁸

Reactie CBP: De bereidheid van Tele2 om de toepassing van data-analysetechnieken op te schorten, en de latere intrekking daarvan, zijn als feiten toegevoegd aan de samenvatting van de zienswijze in het Conceptrapport definitieve bevindingen. De hashingmethode van Tele2 wordt apart beoordeeld. Het CBP komt bij deze beoordeling (kort samengevat) tot de conclusie dat de gebruikte hashing methode niet leidt tot onomkeerbare anonimisering en dat er een risico van heridentificatie is. De wijze waarop Tele2 hasht is een vorm van pseudonimiseren, een technische waarborg ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens als bedoeld in artikel 13 van de Wbp, maar niet van anonimiseren.³⁰⁹ De gegevens over en uit het dataverkeer zijn voor Tele2 direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon, ondanks de gebruikte versleuteling. Omdat Tele2 de data analyse via de [VERTROUWELIJK]-apparatuur niet heeft gestaakt, is er geen sprake van beëindiging van de geconstateerde overtredingen. De zienswijze 1 van Tele2 heeft op dit punt daarom niet geleid tot aanpassing van de conclusies in het rapport.

Zienswijze 1 Tele2: Tele2 brengt in haar zienswijze naar voren dat de inzet van data-analyse om prepaid gebruikers in staat te stellen online hun tegoed op te waarden proportioneel en evenredig was. [VERTROUWELIJK] om de gebruikers in staat te stellen naar een betaalwebsite te surfen. Ondubbelzinnige toestemming van de gebruiker is volgens Tele2 niet vereist om dat het gaat om uitvoering van de overeenkomst van de prepaidklant met Tele2.³¹⁰ Tele2 geeft aan dat zij niettemin

³⁰⁶ Zienswijze 1 Tele2, randnummer 7 e.v.

³⁰⁷ Idem, randnummer 13.

³⁰⁸ Brief van Tele2 van 11 april 2012, p. 3.

³⁰⁹ Naleving van het bepaalde in artikel 13 van de Wbp (beveiliging) valt buiten de scope van dit onderzoek.

³¹⁰ Zienswijze 1 Tele2, randnummers 74 en 77-78.

bereid is te onderzoeken of alsnog toestemming kan worden gevraagd.³¹¹ Bij brief van 11 april 2012 schrijft Tele2 dat van de betreffende analyse-apparatuur "*binnen Tele2 thans geen gebruik meer wordt gemaakt.*"

Reactie CBP: De zienswijze 1 van Tele2 heeft op dit punt geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies. Door het stopzetten en gestopt houden van de data-analysetool voor het opwaarderen van prepaidtegoeden worden voor dit hiervoor genoemde doeleinde thans geen persoonsgegevens die ook verkeersgegevens zijn meer verwerkt en handelt Tele2 (daardoor) niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

³¹¹ Idem, randnummer 79.

Bijlage IV Zienswijze 2 Tele2³¹² op de Concept definitieve bevindingen, met de reactie daarop van het CBP

(zoals weergegeven in het rapport definitieve bevindingen, gegroepeerd én aangevuld in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van het rapport definitieve bevindingen).

Opmerkingen en aanvullingen feitelijk kader

Zienswijze 2 Tele2: In haar zienswijze brengt Tele2 naar voren dat het CBP feitelijke fouten heeft hersteld in het Conceptrapport definitieve bevindingen, maar dat de conclusies van het CBP niet wezenlijk veranderd zijn.³¹³

Reactie CBP: De zienswijze 1 van Tele2 heeft (inderdaad) geleid tot aanpassing van de feitelijke bevindingen in het Conceptrapport definitieve bevindingen, zoals ook weergegeven in **Bijlage III** bij dit rapport. De betreffende zienswijze heeft inderdaad geen aanleiding gegeven tot aanpassing van de conclusies van het CBP. Wel is in dit rapport definitieve bevindingen de beoordeling aangepast van data-analyse voor prepaidverkeer. Bij nader inzien, mede op grond van zienswijze 1 van Tele2 stelt het CBP vast dat de door Tele2 gehanteerde methode proportioneel was, en geen overtreding opleverde van het bepaalde in de Tw, jo. de Wbp.

Zienswijze 2 Tele2: In haar brief van 21 februari 2013 vult Tele2 aan dat de data-analyse technieken niet alleen worden ingezet voor netwerkforecasting in de zin van voorspellen van benodigde netwerkcapaciteit in de nabije toekomst, maar ook voor het overwegen van alternatieven zoals [VERTROUWELIJK].³¹⁴

Reactie CBP: De zienswijze 2 van Tele2 heeft op dit punt geleid tot een aanvulling op het feitelijk kader in het rapport definitieve bevindingen, maar niet tot aanpassing van de conclusies van het rapport.

Zienswijze 2 Tele2: Tele2 illustreert met een aantal voorbeelden dat toenames in het dataverkeer moeilijk voorspelbaar zijn. *"Aanbieders van mobiel internet bevinden zich in terra incognita. (...) De lancering van een nieuw toesteltype of het onverwachte succes van een bepaalde app kan plotseling leiden tot een enorme toename van het dataverkeer."*³¹⁵ Tele2 noemt daarbij gebruikers die kennelijk voorop lopen in het gebruik van nieuwe apps en/of nieuwe toestellen en die daardoor een aanwijzing kunnen vormen voor een significante toename van het dataverkeer. Ook noemt Tele2 de mogelijkheid om terug te kunnen kijken naar dataverbruik per soort toestel.³¹⁶

Reactie CBP: De zienswijze 2 van Tele2 heeft op dit punt geleid tot precisering en inkorting van het feitelijk kader in het rapport definitieve bevindingen. Uit de zienswijze blijkt dat Tele2 de data-analyse apparatuur gebruikt voor het analyseren

³¹² Dit betreft de zienswijze van Tele2 van 30 oktober 2012, zoals aangevuld bij brief van 21 februari 2013.

³¹³ Zienswijze 2 Tele2 van 30 oktober 2012, randnummers 3-5.

³¹⁴ Reactie Tele2 van 21 februari 2013 op vordering inlichtingen CBP, p. 2.

³¹⁵ Zienswijze 2 Tele2, randnummer 11.

³¹⁶ Idem, randnummers 15-16.

van het (volume van) dataverbruik van klanten, en niet om bijvoorbeeld individuele *chatty apps* te kunnen identificeren die mogelijk voor overbelasting zorgen van het radiokanaal. Tele2 is immers een MVNO. Voor het huidige 3G-verkeer maakt zij gebruik van de infrastructuur van T-Mobile. Daardoor heeft Tele2, anders dan andere telecom operators met een eigen infrastructuur van zendmasten, niet te kampen met overbelasting van het radiokanaal door genoemde *chatty apps*. De zienswijze 2 van Tele2 heeft op dit punt niet geleid tot aanpassing van de conclusies van het rapport.

Zienswijze 2 Tele2: Gevraagd door het CBP naar de mogelijkheid van een steekproefsgewijze toetsing van netwerkgebruik, middels een selecte of aselechte steekproef, heeft Tele2 een docent geconsulteerd aan de [VERTROUWELIJK] gespecialiseerd in *social statistics*, [VERTROUWELIJK]. [VERTROUWELIJK] visie luidt (samengevat) als volgt.

Het volgen van een kleine groep klanten (die daartoe toestemming hebben gegeven, een selecte steekproef) leidt waarschijnlijk tot vertekening en wordt daarom door [VERTROUWELIJK] verder niet besproken.

Omdat er sprake is van scheve verdelingspatronen (een relatief klein deel van de klanten verbruikt een groot deel van het datavolume), dient de aselechte steekproef 50% of meer van de klanten te beslaan. Omdat in dit geval klanten door de tijd heen moeten worden gevolgd (longitudinale data), schrijft [VERTROUWELIJK], is de duur en de representativiteit van de steekproef van groot belang. Om het gedrag per klant (datagebruik en type toestel) goed in beeld te krijgen zouden eerst alle klanten een tijd moeten worden gevolgd. In verband met de voortdurende verandering van het klantgedrag, moet de steekproef bovendien minimaal elke zes maanden opnieuw worden genomen. Tele2 acht de steekproefmethode in dit licht, mede gezien de aanzienlijke operationele belasting en kosten, geen verbetering ten opzichte van haar huidige werkwijze.

Reactie CBP: [VERTROUWELIJK] is er (op voorspraak van Tele2) van uitgegaan dat Tele2 voor het doeleinde van netwerkbeheer de beschikking dient te hebben over longitudinale data op individueel, niet-geanonimiseerd niveau. De beschreven alternatieve methodiek leidt in dat geval niet tot een verbetering ten opzichte van de huidige werkwijze. Er bestaan echter andere alternatieven om voor het doeleinde van netwerkbeheer inzicht te krijgen in het (fluctuerend) volume van het dataverkeer, die in paragraaf 3.6.1. van dit rapport nader worden uitgewerkt.

De zienswijze 2 van Tele2 heeft op dit punt geleid tot een aanvulling op het feitelijk kader in het rapport met betrekking tot de mogelijkheid van steekproeven. De zienswijze heeft op dit punt niet geleid tot aanpassing van de conclusies dat er een proportioneel alternatief is voor de huidige werkwijze van Tele2, waarbij de verkeersgegevens zo snel mogelijk onomkeerbaar worden geanonimiseerd.

Spam-, virus en spywarefiltering

Zienswijze 2 Tele2: Tele2 maakt bezwaar tegen opname van het gebruik van spam-, virus- en spywarefiltering van e-mailverkeer in het rapport, omdat dit volgens haar geen relatie heeft met het onderwerp van het onderzoek, de toepassing van *deep packet*

inspection technieken op het mobiele dataverkeer. Tele2 geeft aan dat de filtering louter wordt toegepast op de eigen e-mailservers, en dus niet op e-mails van gebruikers met een account van een andere provider. Niettemin neemt Tele2 nota van het feit dat het CBP erkent dat Tele2 gerechtigd is dergelijke filtering toe te passen, zelfs met toepassing van DPI-technologie, mits Tele2 klanten hierover voldoende informeert.³¹⁷

Reactie CBP: De zienswijze 2 van Tele2 heeft geleid tot een correctie in de feitelijke bevindingen in het rapport met betrekking tot spam-, virus- en spywarefiltering. Ten onrechte nam het CBP aan dat deze analyse betrekking had op al het e-mailverkeer, ook van gebruikers met een e-mailadres bij een andere provider.

De zienswijze 2 van Tele2 heeft echter niet geleid tot het verwijderen van het onderwerp uit het rapport definitieve bevindingen. De scope van het onderzoek van het CBP is niet zozeer gericht op *deep packet inspection*, maar op de toepassing van data-analysetechnieken. Dat Tele2 bij de bestrijding van spam, virussen en spyware de data-analyse alleen toepast op het e-mailplatform en niet op al het mobiele dataverkeer, laat onverlet dat sprake is van data-analyse van de inhoud van communicatieverkeer.

Persoonsgegevens

Zienswijze 2 Tele2: Tele2 gebruikt de informatie niet om individuele abonnees aanbiedingen te doen op basis van de analyse van hun eigen individuele dataverbruik, of voor enige andere gerichte maatregel jegens individuele abonnees.³¹⁸

Reactie CBP: Het is niet het criterium of Tele2 de bedoeling heeft om de gegevens over en uit het dataverkeer of voor dat doeleinde of andere doeleinden te gebruiken, maar of de gegevens daarvoor kunnen worden gebruikt. In de wetsgeschiedenis bij de Wbp is in dat verband opgemerkt: *“Indien het daarentegen mogelijk is de gegevens te gebruiken bij voorbeeld om fraude op te sporen, dan is er sprake van persoonsgegevens. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken, ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt.”*³¹⁹ Het gebruik voor een op de persoon gericht doel is mogelijk.

De zienswijze 2 van Tele2 heeft op dit punt niet geleid tot aanvulling van de feitelijke bevindingen in het rapport, noch tot aanpassing van de conclusies in het rapport dat Tele2 persoonsgegevens verwerkt.

Hashing

Zienswijze 2 Tele2: Volgens Tele2 leidt de versleuteling van de [VERTROUWELIJK: identifiers] ertoe dat de identiteit van de gebruiker niet, of slechts met onevenredige inspanningen, valt te achterhalen.

³¹⁷ Idem, randnummer 6.

³¹⁸ Idem, randnummer 18.

³¹⁹ *Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.*

Dit geldt zowel voor het door het CBP geschetste scenario van ontsleuteling door Tele2 zelf, als voor ontsleuteling door [VERTROUWELIJK: B/A].³²⁰

Volgens Tele2 is ontsleuteling door haarzelf, [VERTROUWELIJK], niet evenredig. De specialistische kennis die dat vergt, is binnen het Tele2 concern niet beschikbaar, [VERTROUWELIJK].³²¹ [VERTROUWELIJK]. Het [VERTROUWELIJK: apparatuur]-systeem voegt volgens Tele2 dus geen nieuwe of wezenlijke grotere risico's toe dan er al bestaan binnen Tele2.³²²

Ten aanzien van ontsleuteling door [VERTROUWELIJK: B/A] schrijft Tele2 dat dit scenario een hoogst theoretisch gehalte heeft, omdat [VERTROUWELIJK].³²³

Bovendien stelt Tele2 dat [VERTROUWELIJK].³²⁴

Reactie CBP: Het CBP heeft in paragraaf 3.3 gemotiveerd beoordeeld dat Tele2 persoonsgegevens verzamelt/verwerkt bij de inzet van data-analysetechnieken op het mobiele dataverkeer en dat de toegepaste hashingmethode niet leidt tot onomkeerbare anonimisering. Het feit dat [VERTROUWELIJK] Tele2 [VERTROUWELIJK] op dit moment zeggen de benodigde kennis niet in huis te hebben om invoer en uitvoer te vergelijken, laat onverlet dat de mogelijkheid wel degelijk bestaat. Evenmin is relevant of er daarnaast nog andere mogelijkheden bestaan om internetgedrag van klanten te volgen. Via de [VERTROUWELIJK]-apparatuur is per klant een overzicht beschikbaar van diens webverkeer, gesorteerd op gebruikte protocollen, geselecteerde hostnames en apps. Dit verschilt wezenlijk van bijvoorbeeld een realtime tap, waarbij grote hoeveelheden ongesorteerde data beschikbaar komen.

Ten aanzien van de [VERTROUWELIJK] verplichtingen (van [VERTROUWELIJK]) geldt dat dit een goede manier is om te voldoen aan de verplichting om naast technische ook organisatorische beveiligingsmaatregelen te treffen. Deze afspraken laten onverlet dat van persoonsgegevens sprake is. [VERTROUWELIJK].

Technisch is sprake van pseudonimisering, niet van anonimisering. Dit volgt ook mede uit het doeleinde van Tele2 om voor netwerkbeheer en marktonderzoeksdoeleinden het individuele gedrag van een klant door de tijd heen (gemiddeld twaalf maanden lang) te kunnen volgen. Het toepassen van pseudoniemen kan een goede invulling zijn van om beveiligingsrisico's te verkleinen, zeker nu sprake is van doorgifte van de gegevens naar landen zonder adequaat beschermingsniveau, maar kan niet leiden tot de conclusie dat van persoonsgegevens geen sprake is.

De zienswijze van Tele2 heeft ten aanzien van de beoordeling of na hashing nog sprake is van verwerking van persoonsgegevens, niet geleid tot aanpassing van de conclusies van het rapport.

³²⁰ Zienswijze 2 Tele2, randnummers 30-39.

³²¹ Idem, randnummer 32.

³²² Idem, randnummer 34.

³²³ Idem, randnummer 36.

³²⁴ Idem, randnummers 37-38.

Zienswijze 2 Tele2: Volgens Tele2 blijkt uit de overwegingen van de Artikel 29-werkgroep in advies 4/2007 over het begrip persoonsgegevens "(i) dat gebruik van niet-geaggregeerde statistische gegevens zo kan worden ingericht dat geen sprake is van persoonsgegevens, (ii) dat hashing daarbij een rol kan spelen, en (iii) dat bij de beoordeling of heridentificatie mogelijk is, de waarschijnlijkheid daarvan moet worden meegewogen en niet kan worden volstaan met het identificeren van theoretische mogelijkheden to heridentificatie."³²⁵ Ook stelt Tele2 dat volgens de Artikel 29-werkgroep bij eenrichtingsversleuteling over het algemeen geanonimiseerde gegevens ontstaan. De door Tele2 toegepaste hashing is volgens Tele2 een vorm van eenrichtingsversleuteling die dus in beginsel leidt tot anonieme data waarop de Wbp niet langer van toepassing is.³²⁶ Ten aanzien van tweerichtingsversleuteling geeft de Artikel 29-werkgroep een voorbeeld (voorbeeld 17) waarin het gaat om de verwerking van niet-geaggregeerde statistische gegevens, die met een sleutel zijn terug te leiden tot geïdentificeerde individuen. Volgens de Artikel 29-werkgroep kunnen ook op die wijze herleidbare gegevens in sommige gevallen voor de ontvanger geen persoonsgegevens zijn, afhankelijk van de getroffen waarborgen. "In dat kader wijst Tele2 erop dat het advies op p. 21 ook uitdrukkelijk de toepassing van onomkeerbare hashing noemt als een voorbeeld van een passende technische maatregel om identificatie te voorkomen. Is daarvoor gekozen, maar is desondanks door onvoorziene omstandigheden toch heridentificatie mogelijk, dan is dat volgens de Art. 29 Groep geen reden om alle gehashte informatie als persoonsgegevens te beschouwen, nu heridentificatie niet redelijkerwijs te verwachten was."³²⁷

Reactie CBP: In algemene zin is bij inschakeling van een TTP/onaafhankelijke derde die een cryptografische sleutel bewaart of een cryptografische module beheert sprake van beveiligingsmaatregel van gegevensscheiding. In beginsel is gegevensscheiding een passende beveiligingsmaatregel, maar gegevensscheiding betekent niet dat de betreffende gegevens niet meer gelden als persoonsgegevens. Alleen in uitzonderlijke omstandigheden, zoals de waarborg van een medisch beroepsgeheim, kan een dergelijke gegevensscheiding ertoe leiden dat niet langer sprake is van persoonsgegevens voor de ontvanger. Het gaat hier echter niet om beoordeling van de resultante van de hashing voor de ontvanger, maar om de beoordeling of sprake is van persoonsgegevens. Zoals vastgesteld in par 3.3, onder het kopje 'Hashing', is de facto geen sprake van onomkeerbare anonimisering, [VERTROUWELIJK] Daar komt nog eens bij dat het doeleinde van de verwerking door Tele2 gericht is op het waarnemen en vastleggen van individueel gedrag door de tijd heen. De gegevensverwerking is (dus) mede gericht op individualisering, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

De zienswijze 2 van Tele2 heeft ten aanzien van de beoordeling of na hashing nog sprake is van verwerking van persoonsgegevens (tevens verkeersgegevens), geleid tot uitbreiding van de beoordeling van hashing in het rapport, maar niet tot aanpassing van de conclusies van het rapport.

³²⁵ Idem, randnummer 43.

³²⁶ Idem, randnummer 45.

³²⁷ Idem, randnummer 47.

Zienswijze 2 Tele2: Tele2 heeft het CBP bij brief van 21 februari 2013 een prijsopgave gestuurd van leverancier [VERTROUWELIJK: A] [VERTROUWELIJK].³²⁸

Reactie CBP: De hashes en bijkomende gegevens blijven ook in de voorgestelde nieuwe werkwijzen persoonsgegevens. [VERTROUWELIJK]. Door deze werkwijze is Tele2 in staat om het gedrag per klant door de tijd heen te volgen, door telkens nieuwe gegevens over en uit het dataverkeer aan de [VERTROUWELIJK] hashwaarde per klant te koppelen. [VERTROUWELIJK]

Netwerkbeheer

Zienswijze 2 Tele2: Volgens Tele2 is het oordeel van het CBP dat er andere, minder ingrijpende alternatieven zouden bestaan, onjuist. Verwijdering of anonimisering van de persoonsgegevens leidt ertoe dat het niet meer mogelijk is individuele gebruikspatronen van elkaar te onderscheiden. Volgens Tele2 is het voor netwerkbeheer noodzakelijk om dataverbruik te kunnen waarnemen op individueel niveau, door de tijd heen, om trends te kunnen waarnemen en te kunnen anticiperen op veranderingen in het dataverkeer over tijd. Deze informatie kan aanleiding zijn om de netwerkcapaciteit uit te breiden, of te bezien of de beprijzing van datadiensten moet worden aangepast.³²⁹ Tele2 schrijft: *“Verwijdering van persoonsgegevens leidt praktisch gezien tot aggregatie van informatie. Dat zou ertoe leiden dat Tele2 nog wel kan zien dat er in augustus 2012 15.483 keer gebruik is gemaakt van een nieuwe voice-over-IP app op het netwerk van Tele2, en dat dit in oktober is toegenomen tot 133.788 keer, maar niet of het daarbij gaat om dezelfde abonnees die de betreffende app steeds vaker gebruiken of een toename in het aantal abonnees dat de app gebruikt. Evenmin is zichtbaar of dat gebruik per abonnee over tijd toeneemt, afneemt of stabiel blijft. De alternatieven van het CBP leiden dus tot een aanmerkelijke verschraling van de informatie die Tele2 beschikbaar komt. Uit oogpunt van netwerkbeheer is geen sprake van gelijkwaardige resultaten, die voor Tele2 net zo informatief zijn als het gaat om de vraag of de waargenomen verkeerspatronen wel of geen nieuwe investeringen rechtvaardigen.”*³³⁰

Aanvullend schrijft Tele2 in haar brief van 21 februari 2013 dat het voor Tele2 zaak is om in haar analyse het verschil te kunnen zien tussen enerzijds incidenten en anderzijds structurele trends of ontwikkelingen, aangezien deze om een andere respons vragen. [VERTROUWELIJK]

Reactie CBP: De noodzaak om (een beperkte set) gegevens over het dataverkeer te verzamelen behelst niet zonder meer een noodzaak om de aldus verkregen gegevens vervolgens ook op individueel niveau vast te leggen en gedurende twaalf maanden te bewaren. Getoetst moet worden of ook deze verwerking voldoet aan het proportionaliteits- en subsidiariteitsvereiste. Dat wil zeggen, of het doeleinde niet anderszins of met minder ingrijpende middelen worden bereikt en of de inbreuk op de belangen van de bij de verwerking betrokkenen evenredig is in verhouding tot het met de verwerking te dienen doel.

³²⁸ Reactie Tele2 van 21 februari 2013 op vordering inlichtingen CBP, p. 7 en 8.

³²⁹ Idem, randnummers 21 en 24.

³³⁰ Idem, randnummer 24.

De aard van de verzamelde persoonsgegevens, de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor gegevensvergaring in de vorm van data-analyse technieken naar aanleiding van het gebruik van het netwerk van de aanbieders en het risico (kans x impact) voor de betrokkenen van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, spelen een rol in de belangenafweging. Daarnaast worden de inspanning en kosten meegewogen die voor Tele2 gepaard gaan met de ontwikkeling en implementatie van (technische) mogelijkheden om hetzelfde doel op een andere, minder inbreukmakende wijze te bereiken, evenals de consequenties voor de continuïteit en integriteit van haar netwerk.

Het CBP begrijpt dat het voor het netwerkbeheer van Tele2 handig kan zijn om individueel gedrag door de tijd heen te kunnen volgen, maar daarmee is de gevolgde specifieke data-analyse methode met behulp van de [VERTROUWELIJK]-apparatuur niet automatisch ook noodzakelijk en daarmee gerechtvaardigd. [VERTROUWELIJK]. Om vast te stellen of bepaalde types toestellen meer datagebruik veroorzaken dan anderen hoeft Tele2 derhalve geen persoonsgegevens vast te leggen en te bewaren. Ten aanzien van individueel gebruik van specifieke protocollen, apps en websites heeft Tele2 onvoldoende onderbouwd en aannemelijk gemaakt waarom het voor haar noodzakelijk zou zijn voor netwerkbeheer om onderscheid te kunnen maken tussen het gedrag van individuele gebruikers. Immers, ongeacht de vraag of 1 gebruiker honderd keer per dag naar een specifieke website of app gaat, of dat honderd gebruikers dat 1 maal per dag doen, heeft Tele2 voldoende capaciteit nodig op haar netwerk om dit verkeer te kunnen overbrengen. Indien het aantal dagelijkse bezoeken aan een website of app steeds toeneemt, kan Tele2 een inschatting maken van benodigde netwerkcapaciteit of andere door haar genoemde mogelijke interventie maatregelen treffen, zoals [VERTROUWELIJK]. Dergelijke ontwikkelingen met betrekking tot het datavolume kunnen heel goed uit geaggregeerde gegevens worden opgemaakt.

Uit het onderzoek is gebleken dat huidige bij Tele2 in gebruik zijnde [VERTROUWELIJK: apparatuur]-apparatuur technisch ook in staat is om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren. Hetzelfde doel, het verkrijgen van verkeersstatistieken voor netwerkbeheer, kan dus op een andere, minder inbreukmakende wijze worden bereikt.

Ten aanzien van de risico's voor betrokkenen dat er op inbreuk wordt gemaakt op hun persoonlijke levenssfeer geldt het volgende. 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 oneigenlijk gebruik van gegevens te voorkomen, (beveiligings)incidenten niet altijd kunnen worden voorkomen. Het hashen van het [VERTROUWELIJK: identifier] is wel een waarborg ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp. Maar gelet op de aard van de verzamelde persoonsgegevens bieden andere maatregelen dan het zo snel 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.

De zienswijze 2 van Tele2 heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het rapport dat een alternatief voor de door Tele2 ingezette data-analysetools dat ervoor zorgt dat de verkeersgegevens direct onomkeerbaar worden geanonimiseerd op dit moment proportioneel is.

Marktonderzoeksdoeleinden

Zienswijze 2 Tele2: Tele2 herhaalt dat zij de in het kader van netwerkbeheer verzamelde gegevens niet gebruikt voor het soort marketingdoeleinden waarvoor toestemming is vereist, zoals omschreven in artikel 11.5, derde lid, onder a, van de Tw. Daarbij licht Tele2 toe dat als uit de analyse van verbruiksdata blijkt dat gebruikers met een bepaald abonnementsvorm of toestel zoveel data verbruiken dat daardoor congestie optreedt, dat Tele2 dan de voorwaarden voor die abonnementsvorm of behorend bij dat toesteltype kan aanpassen voor nieuwe abonnees.³³¹

Reactie CBP: Het CBP begrijpt uit de zienswijze 2 van Tele2 dat zij een onderscheid maakt tussen direct marketing (verkoopactiviteiten) en marktonderzoek (ten behoeve van het bepalen van de prijsstelling van bestaande producten en diensten, en het ontwikkelen van nieuwe diensten). Artikel 11.5, derde lid, van de Tw vereist echter toestemming van de betrokkenen voor zowel marktonderzoek als verkoopactiviteiten met betrekking tot elektronische communicatiediensten.

Als hoofdregel geldt op grond van artikel 11.5 van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie (inclusief de afgeleide doeleinden verkeersbeheer en behandeling van verzoeken om inlichtingen van klanten etc.). 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.

³³¹ Zienswijze 2 Tele2, randnummer 56.

De zienswijze 2 van Tele2 leidt op het punt van marktonderzoeksdoeleinden niet tot aanvulling van de feitelijke bevindingen en aanpassing van de bijbehorende conclusies van het rapport.

Meld- en informatieplicht

Zienswijze 2 Tele2: In reactie op de beoordeling van het CBP dat de melding van Tele2 bij het CBP onvolledig is, en dat Tele2 in strijd handelt met de informatieplicht uit de artikelen 33 en 34 Wbp, heeft Tele2 twee conceptteksten bij haar zienswijze 2 gevoegd; een aanvulling van de melding (Bijlage 2 bij Zienswijze 2) en een toevoeging aan het privacystatement (Bijlage 3 bij Zienswijze 2).³³²

Reactie CBP: De conceptteksten leiden tot aanvulling van het feitelijk kader van het rapport met betrekking tot de melding en de informatie. De conceptteksten worden tevens besproken in de beoordeling, maar leiden, omdat het alleen nog concepten betreft, niet tot aanpassing van de conclusies van het rapport.

Bewerkersovereenkomst en doorgifte

Zienswijze 2 Tele2: Tele2 betwist dat een bewerkersovereenkomst noodzakelijk zou zijn, maar heeft als bijlage 1 bij haar zienswijze 2 een conceptovereenkomst bijgevoegd tussen [VERTROUWELIJK], met [VERTROUWELIJK].³³³

Ook ten aanzien van de beoordeling dat Tele2 door doorgifte van persoonsgegevens via [VERTROUWELIJK: A] in strijd handelt met artikel 76 Wbp, handhaaft Tele2 haar standpunt dat geen sprake is van (doorgifte van) persoonsgegevens, maar biedt Tele2 niettemin aan, indien nodig, een modelbepaling aan te gaan voor doorgifte, zoals goedgekeurd door de Europese Commissie.³³⁴ Een concept overeenkomst is als bijlage gevoegd bij haar zienswijze 2. Het betreft een concept doorgifte-overeenkomst tussen [VERTROUWELIJK], op basis van de model doorgiftgebepalingen van de Europese Commissie, waarbij Tele2 [VERTROUWELIJK] als verantwoordelijke optreedt, en [VERTROUWELIJK: A] als bewerker.

Reactie CBP: Beide bijlages worden genoemd en (het bestaan ervan) daarmee toegevoegd aan het feitelijk kader van het rapport. De bijlages hebben echter niet geleid tot aanpassing van de conclusies in het rapport dat na de hashing, ook na eventuele ondertekening van de concept nieuwe overeenkomsten, nog sprake is van van persoonsgegevens, tevens verkeersgegevens.

Door het aangaan van de overgelegde concept bewerkersovereenkomst zal de geconstateerde overtreding van artikel 14 van de Wbp (bewerkersovereenkomst) worden beëindigd voor wat betreft de relatie met haar bewerker [VERTROUWELIJK: A]. Voor wat betreft de relatie met haar bewerker [VERTROUWELIJK: B] zal door het aangaan van de overgelegde concept bewerkersovereenkomst de geconstateerde overtreding van artikel 14 van de Wbp worden beëindigd indien en voor zover de concept bewerkersovereenkomst wordt aangevuld met de categorieën van verwerkte persoonsgegevens, de doeleinden (de opdracht aan [VERTROUWELIJK:

³³² Idem, randnummers 62 en 63.

³³³ Idem, randnummer 64.

³³⁴ Idem, randnummer 67.

B]/verwerkings handelingen) en afspraken over het al dan niet toestaan van verwerking door subbewerkers.

Door gebruik te maken van een door beide partijen getekende versie van de overgelegde concept doorgifte-overeenkomst tussen Tele2 [VERTROUWELIJK] en [VERTROUWELIJK: A], aangevuld met een ingevulde Appendix 2, zal de geconstateerde overtreding van artikel 76 van de Wbp (doorgifte) worden beëindigd.