

## **College bescherming persoonsgegevens**

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

Z2011-00462

Rapport definitieve bevindingen

Mei 2013 met corrigendum van 20 juni 2013

**OPENBARE VERSIE**

## Inhoudsopgave

|                                                                                                    |            |
|----------------------------------------------------------------------------------------------------|------------|
| <b>Samenvatting.....</b>                                                                           | <b>3</b>   |
| <b>1. Inleiding .....</b>                                                                          | <b>6</b>   |
| <b>2. Feitelijke bevindingen .....</b>                                                             | <b>16</b>  |
| 2.1 Organisatiebeschrijving .....                                                                  | 16         |
| 2.2 Mobiel netwerk, netwerkverkeer, plaatsing data-analyse apparatuur en opbouw datapakketten..... | 18         |
| 2.3 Overzicht doeleinden.....                                                                      | 20         |
| 2.4 Verkeersbeheer.....                                                                            | 22         |
| 2.5 Facturering.....                                                                               | 37         |
| 2.6 Beveiliging .....                                                                              | 42         |
| 2.7 Behandeling van verzoeken om inlichtingen van klanten.....                                     | 44         |
| 2.8 Verdere verwerking .....                                                                       | 46         |
| <b>3. Uitwerking van het wettelijk kader en beoordeling .....</b>                                  | <b>48</b>  |
| 3.1 Wettelijk kader: samenloop Wbp en Tw .....                                                     | 48         |
| 3.2 Verantwoordelijke .....                                                                        | 49         |
| 3.3 Verwerking van persoonsgegevens .....                                                          | 50         |
| 3.4 Verkeersgegevens versus communicatie .....                                                     | 58         |
| 3.5 Gegevensverwerking .....                                                                       | 63         |
| 3.6 Grondslag .....                                                                                | 64         |
| 3.6.1 Verkeersbeheer.....                                                                          | 76         |
| 3.6.2 Facturering (prepaidverkeer).....                                                            | 84         |
| 3.6.3 Firewalls, spamfilters en virusscanners.....                                                 | 87         |
| 3.6.4 Behandeling van verzoeken om inlichtingen van klanten.....                                   | 89         |
| 3.7 Verdere verwerking .....                                                                       | 90         |
| 3.8 Uitdrukkelijk omschreven en gerechtvaardigde doeleinden.....                                   | 91         |
| 3.9 Informatieplicht .....                                                                         | 95         |
| 3.10 Meldplicht.....                                                                               | 100        |
| <b>4. Conclusies .....</b>                                                                         | <b>101</b> |

### Bijlagen:

- I. Overzicht 3G netwerkarchitectuur
- II. Overzicht verwerkte gegevens, per doeleinde
- III. Verklarende woordenlijst

- IV. Zienswijze 1 Vodafone, met de reactie daarop van het CBP
- V. Zienswijze 2 Vodafone, met de reactie daarop van het CBP

## SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft onderzoek gedaan naar hoe Vodafone *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 Vodafone hierbij persoonsgegevens verwerkt en zo ja, of Vodafone 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-analyse technieken in te zetten is netwerkbeheer, om te zorgen dat het mobiele netwerk goed functioneert en niet overbelast raakt. Daarnaast gebruiken bedrijven de technieken voor andere doeleinden, zoals facturering, marktonderzoek, blokkering van bepaalde internettoepassingen, spam- en virusfiltering en klachtafhandeling.

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

### Data-analyse bij Vodafone

Vodafone verwerkt gegevens over en uit het dataverkeer van circa 3,2 miljoen Vodafone abonnees met mobiel internet, voor de dienstverlening aan haar klanten. 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.

Vodafone verwerkt de persoonsgegevens voor de volgende onderzochte doeleinden:

- verkeersbeheer en facturering (netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van verkeer van prepaid klanten naar (gratis) opwaardeersites);
- beveiliging (specifiek: spam- en virusfiltering en malwarebestrijding); en
- behandeling van verzoeken om inlichtingen van klanten.

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

### Geconstateerde overtredingen

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



### Overtredingen die nog niet zijn beëindigd

#### *Meldingsplicht*

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen wettelijk verplicht deze gegevensverwerking te melden bij het CBP. De huidige melding van Vodafone is niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking. Vodafone is hierdoor in overtreding.

Vodafone heeft aangegeven bereid te zijn wijzigingen door te voeren in de melding bij het CBP.

### Overtredingen die gedeeltelijk zijn beëindigd

#### *Verkeersbeheer en facturering*

Omdat Vodafone voor het detecteren en oplossen van problemen in het netwerk bij aanvang van het onderzoek de persoonsgegevens niet zo snel mogelijk na het verzamelen verwijderde, was het bedrijf in overtreding.

Naar aanleiding van het onderzoek heeft Vodafone de bewaartermijnen van de persoonsgegevens voor netwerkmonitoring aanzienlijk verkort. Door deze getroffen maatregel zijn de geconstateerde overtredingen gedeeltelijk beëindigd. Op één punt is de bewaartermijn van persoonsgegevens voor netwerkmonitoring nog te lang.

#### *Informeren abonnees*

Vodafone 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. Vodafone informeerde abonnees bij aanvang van het onderzoek niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking bij de toepassing van data-analyse technieken. Daarnaast informeerde Vodafone hen niet over de categorieën van verwerkte persoonsgegevens en de duur van de verwerking (bewaartermijnen). Vodafone was hierdoor in overtreding.

Vodafone heeft de privacyverklaring van het bedrijf per augustus 2012 aangepast. Door deze getroffen maatregel zijn de geconstateerde overtredingen gedeeltelijk beëindigd. Er ontbreekt echter nog informatie over de bewaartermijnen.

### Overtredingen die zijn beëindigd

#### *Verkeersbeheer en facturering*

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

Omdat Vodafone voor netwerkplanning [VERTROUWELIJK: apparatuur] gebruikte dat de verzamelde persoonsgegevens niet zo snel mogelijk verwijderde, was het bedrijf in overtreding.

Vodafone heeft het CBP, na het sluiten van het onderzoek, medegedeeld dat dit apparaat sinds vorig jaar niet meer in gebruik is. Het CBP heeft dit niet nader onderzocht. Voor zover Vodafone het apparaat sindsdien niet meer gebruikt, zijn de geconstateerde overtredingen op dit punt beëindigd.

#### *Verkeersbeheer en facturering*

Om prepaid abonnees in staat te stellen opwaardeersites te bezoeken als hun tegoed op is, verwerkte Vodafone bij aanvang van het onderzoek URL's om de (gratis) opwaardeersites te herkennen. Dit terwijl er ook andere mogelijkheden waren. Omdat deze gegevensverwerking onevenredig was, was Vodafone hierdoor in overtreding.

Vodafone verleent thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK]. Door deze getroffen maatregel zijn de geconstateerde overtredingen op dit punt beëindigd.

#### Geen overtredingen geconstateerd

#### *Verkeersbeheer en facturering*

Vodafone gebruikt voor netwerkplanning verder [VERTROUWELIJK: apparatuur] dat de persoonsgegevens wel zo snel mogelijk onomkeerbaar anonimiseert. Voor de inzet van dit apparaat heeft het bedrijf een wettelijke grondslag. Op dat punt is Vodafone dan ook niet in overtreding (geweest). Vodafone heeft naar aanleiding van het onderzoek bovendien de bewaartermijnen van de geanonimiseerde gegevens verkort.

#### *Video-optimalisatie, spam- en virusfiltering & malwarebestrijding en klachtbehandeling*

Vodafone heeft ook een wettelijke grondslag voor de verwerking ten behoeve van video-optimalisatie, spam- en virusfiltering & malwarebestrijding en behandeling van verzoeken om inlichtingen van klanten. Op deze punten is Vodafone dan ook niet in overtreding (geweest).

## 1. INLEIDING

Het College bescherming persoonsgegevens (CBP) heeft op grond van artikel 60 van de Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek ingesteld naar de wijze waarop Vodafone Libertel B.V. (hierna: Vodafone) in haar mobiele netwerk *packet inspection* technologie en technieken (hierna: data-analyse technieken) toepast.

Het CBP heeft onderzocht of Vodafone hierbij persoonsgegevens verwerkt en zo ja, of Vodafone 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

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

### Aanleiding onderzoek

Mobiele netwerken bestaan vandaag de dag vaak uit een of meer GSM-gedeeltes (voor de afhandeling van spraakverkeer) en GPRS/UMTS-gedeeltes (voor de afhandeling van dataverkeer).<sup>1</sup> 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).<sup>2</sup> Spraak-, data- en signaleringsverkeer maken gebruik van dezelfde radioweg (toegang tot het mobiele netwerk). Elk onderdeel van het mobiele netwerk heeft een maximum capaciteit.

Smartphones verbreken veelvuldig de verbinding om de batterij te sparen. Er zijn applicaties (*apps*) die vaak weer verbinding (doen) zoeken met het netwerk, om gegevens te verversen door data van de server af te halen of te checken of er updates beschikbaar zijn. Dit fenomeen wordt wel '*chatty apps*' genoemd en leidt tot een significante toename van het signaleringsverkeer. Als het radiotoegangsnetwerk crasht als gevolg van teveel signaleringen in het GPRS- of UMTS-gedeelte kan er ook niet meer worden gebeld.

---

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

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

Een belangrijke reden voor veel mobiele netwerkaanbieders om data-analyse technieken in te zetten is netwerkbeheer, om problemen in het netwerk te detecteren en op te lossen en om de gevolgen van congestie te beperken.<sup>3</sup>

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

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

---

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

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

<sup>4</sup> 'OPTA jaarverslag en marktmonitor 2011', *Nieuwsbericht OPTA* 23 april 2012. URL: <https://www.acm.nl/nl/publicaties/publicatie/10347/OPTA-jaarverslag-en-marktmonitor-2011/>. Presentatie marktmonitor 2011, *Presentatie OPTA* 23 april 2012. URL: <https://www.acm.nl/nl/publicaties/publicatie/10346/Presentatie-marktmonitor-2011/>.

<sup>5</sup> "Het totaal aantal aansluitingen met mobiel breedband is eind 2012 ruim 10 miljoen: 9,1 miljoen mobiele telefoons en 1,2 miljoen tablets en dongels." 'Telecommonitor 2012: Lagere omzet voor mobiele aanbieders door minder sms'jes', *Nieuwsbericht OPTA* 17 april 2013. URL: <https://www.acm.nl/nl/publicaties/publicatie/11338/Telecommonitor-2012-Lagere-omzet-voor-mobiele-aanbieders-door-minder-smsjes/>. Zie ook Openbare rapportage mobiel Q4 2012, p. 1. URL: <https://www.acm.nl/nl/download/bijlage/?id=10942> (URL's laatst bezocht op 29 mei 2013).

<sup>6</sup> Van de totaal 22.098.000 mobiele aansluitingen aan het eind van 2012 in Nederland, waren er 9.063.000 met mobiel breedbandinternet en 1.185.000 specifieke mobiele breedbandinternet aansluitingen, zoals tablets en dongels. In totaal 10.248.000 mobiele internetaansluitingen, ofwel 46,4 procent van het totaal aantal mobiele aansluitingen. Tabel "Mobiel: Aantal retailaansluitingen" uit de Openbare rapportage mobiel Q4 2012, p. 1. Het feitelijke percentage smartphone abonnees met internettoegang verschilt per mobiele aanbieder. Vgl. 'Consumenten kopen handset in winkel, bestellen sim online', *Telecompaper* 11 juli 2012. URL: <http://www.telecompaper.com/nieuws/consumenten-kopen-handset-in-winkel-bestellen-sim-online>. Vgl. ook 'Marktrapportage elektronische communicatie (MEC) eerste helft 2012 is uit', *TNO* 18 februari 2013. URL: [http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item\\_id=2013-02-18%2016:42:09.0](http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2013-02-18%2016:42:09.0) (URL's laatst bezocht op 29 mei 2013). Op basis van het aantal aansluitingen voor mobiele telefonie ligt het marktaandeel van Vodafone volgens de Openbare rapportage mobiel Q4 2012 aan het eind van 2012 tussen 25 en 30 procent. Openbare rapportage mobiel Q4 2012, p. 2.

marktaandeel van bijna 2,5% van de mobiele telefonieaansluitingen met een data abonnement.<sup>7</sup>

OPTA heeft in mei en juni 2011 onderzoek (een *quick scan*) uitgevoerd onder de vier grootste mobiele netwerkaanbieders in Nederland (KPN, Vodafone, T-Mobile en Tele2) naar de vraag of en zo ja, hoe deze partijen hun dataverkeer analyseren. OPTA heeft geconcludeerd dat er in dat stadium op basis van de Tw geen aanleiding was voor handhavend optreden.<sup>8</sup> OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van het Samenwerkingsprotocol CBP-OPTA van 12 juli 2005 (hierna: Samenwerkingsprotocol CBP-OPTA).<sup>9</sup>

### 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.<sup>10</sup>

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 en krachtens de wet bepaalde. Dit betekent dat het Cbp een algemene toezichtsbevoegdheid heeft die zich niet alleen uitstrekt tot de naleving van het bij en krachtens het voorstel voor een Wet bescherming persoonsgegevens bepaalde, maar ook tot hetgeen bij en 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.”<sup>11</sup>*

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

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

<sup>9</sup> *Stcrt.* 2005, 133.

<sup>10</sup> *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 53-54.

<sup>11</sup> *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

OPENBARE VERSIE Rapport definitieve bevindingen 29 mei 2013

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

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

Daarnaast is Agentschap Telecom, onderdeel van het ministerie van Economische Zaken (hierna: Agentschap Telecom), voor zover voor dit onderzoek van belang, op grond van artikel 15.1, eerste lid, onder c, h, j en k, van de Tw belast met het toezicht op de naleving van het bepaalde bij of krachtens de Tw, voor zover het onder andere betreft de bepalingen die betrekking hebben op prioritering van alarmnummers als bedoeld in artikel 7.7, derde of vierde lid, het gebruik van verkeersgegevens en locatiegegevens als geregeld in artikel 11.5, artikel 11.5a onderscheidenlijk artikel 11.13, buitengewone omstandigheden als geregeld in hoofdstuk 14 en verdere onderwerpen als bedoeld in de artikelen 11a.1 en 11a.2 (nieuw).<sup>12</sup> 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 Vodafone verzamelt en verwerkt persoonsgegevens, zoals gedefinieerd in artikel 1, aanhef en onder a, van de Wbp?
- Zijn de doeleinden waarvoor Vodafone 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 Vodafone als bedoeld in artikel 8 van de Wbp?
- Heeft Vodafone de betrokkenen (tijdig) geïnformeerd over de gegevensverwerking, zoals bepaald in artikel 34 van de Wbp?
- Heeft Vodafone de verwerking van deze gegevens over en uit het dataverkeer bij het CBP gemeld in de zin van artikel 27 jo. 28 van de Wbp?

---

*van hoofdstuk 11 Telecommunicatiewet betreft, ook op die bepalingen. Daarnaast is het college [van OPTA, toevoeging door het CBP] op basis van hoofdstuk 15 Telecommunicatiewet belast met het toezicht op hoofdstuk 11 Telecommunicatiewet als geheel [behoudens het bepaalde in artikel 15.1, eerste lid, onder h, van de Tw, toevoeging door het CBP]. De nadruk in het toezicht van het college ligt echter op andere aspecten van hoofdstuk 11 Telecommunicatiewet dan die waarop het CBP toeziet." Zie ook Kamerstukken I 2003/04, 28 851, nr. C, p. 34; Kamerstukken II 2002/03, 28 851, nr. 7, p. 43 en Kamerstukken II 1997/98, 25 533, nr. 5, p. 117.*

<sup>12</sup> Zie artikel 2 van het Besluit aanwijzing toezichthouders Telecommunicatiewet. Artikel 1, derde lid, van de Samenwerkingsovereenkomst Agentschap Telecom-College bescherming persoonsgegevens van 15 september 2009 (hierna: Samenwerkingsovereenkomst Agentschap Telecom-CBP) bepaalt, voor zover voor dit onderzoek van belang, dat indien het CBP tijdens onderzoeken in een ander kader op overtredingen van de Tw jo. de Wet bewaarplicht telecommunicatiegegevens stuit, het CBP zelfstandig onderzoek kan verrichten. *Stcrt.* 2009, 13672.

## Verloop onderzoek

OPTA heeft in mei 2011 onderzoek (een quick scan) ingesteld onder de vier grootste mobiele netwerkaanbieders (KPN, Vodafone, T-Mobile en Tele2) naar de vraag of de manier waarop de mobiele netwerkaanbieders datapakketten analyseren strijdig is met bepalingen uit de Tw.<sup>13</sup>

OPTA heeft op 30 juni 2011 haar voorlopige bevindingen gepubliceerd.<sup>14</sup>

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

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

Bij brief van 18 augustus 2011 heeft het CBP schriftelijk inlichtingen ingewonnen bij Vodafone. Bij brief van 22 augustus 2011 heeft Vodafone uitstel verzocht van de termijn voor het geven van deze inlichtingen tot en met 12 september 2011. Het CBP heeft bij brief van 1 september 2011 dit uitstel verleend. Vodafone heeft de gevraagde inlichtingen op 12 september 2011 aan het CBP verstrekt.

Bij brief van 11 oktober 2011 heeft het CBP aanvullende schriftelijke inlichtingen ingewonnen bij Vodafone. Bij brief van 13 oktober 2011 heeft Vodafone uitstel verzocht van de termijn voor het geven van deze inlichtingen tot en met 24 oktober 2011. Het CBP heeft bij brief van 13 oktober 2011 dit uitstel verleend. Vodafone heeft de gevraagde inlichtingen op 24 oktober 2011 aan het CBP verstrekt.

Het CBP heeft Vodafone bij brief van 14 oktober 2011 aangekondigd een onderzoek ter plaatse te zullen uitvoeren bij Vodafone. Op 26 oktober 2011 heeft het onderzoek ter plaatse plaatsgevonden ten kantore van Vodafone in Maastricht. Tijdens genoemd onderzoek heeft het CBP mondeling inlichtingen ingewonnen bij de [VERTROUWELIJK], de [VERTROUWELIJK] en [VERTROUWELIJK]<sup>15</sup> alsmede een aantal (kopieën van) bescheiden gevraagd. Daarnaast heeft het CBP gebruikersinterfaces bekeken van de apparatuur die Vodafone inzet voor data-analyse.

---

<sup>13</sup> 'Voorlopige bevindingen OPTA over gebruik Deep Packet Inspection', *Nieuwsbericht OPTA* 30 juni 2011. URL:

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

<sup>14</sup> 'Voorlopige bevindingen over gebruik Deep Packet Inspection', *Onderzoek OPTA* 30 juni 2011. URL: <https://www.acm.nl/nl/publicaties/publicatie/10234/Voorlopige-bevindingen-over-gebruik-Deep-Packet-Inspection/> (URL laatst bezocht op 29 mei 2013).

<sup>15</sup> Allen gevolmachtigd om tijdens dit onderzoek ter plaatse namens Vodafone het woord te voeren.

Het CBP heeft een aantal (kopieën van) bescheiden meegenomen, in de vorm van 1 USB-stick van 1 GB en 13 print-outs van 1 A4.<sup>16</sup> Vodafone heeft de overige gevraagde antwoorden en (kopieën van) bescheiden (zoals genoemd in de brief van het CBP van 27 oktober 2011) gedeeltelijk op 28 oktober 2011 aan het CBP verstrekt.

Bij e-mail van 28 oktober 2011 heeft Vodafone uitstel verzocht van de termijn voor het geven van de resterende antwoorden en (kopieën van) bescheiden tot 14 november 2011. Het CBP heeft bij brief van 1 november 2011 uitstel verleend tot en met 10 november 2011. Vodafone heeft een deel van de resterende gevraagde antwoorden en (kopieën van) bescheiden (zoals genoemd in de brief van het CBP van 27 oktober 2011) op 10 november 2011 aan het CBP verstrekt.

Bij brief van 10 november 2011 heeft het CBP Vodafone verzocht de ontbrekende antwoorden en (kopieën van) bescheiden alsnog uiterlijk op 14 november 2011 aan het CBP te verstrekken. Bij e-mail van 11 november 2011 heeft Vodafone uitstel verzocht van de termijn voor het geven van deze antwoorden en (kopieën van) bescheiden tot 21 november 2011. Het CBP heeft dit uitstel bij brief van 11 november 2011 verleend.

Vodafone heeft de ontbrekende antwoorden en (kopieën van) bescheiden op 14, respectievelijk 21 en 24 november 2011 aan het CBP verstrekt.

Op 5 december 2011 heeft het CBP mondeling (bevestigd per e-mail) inlichtingen ingewonnen bij Vodafone. Vodafone heeft de gevraagde inlichtingen op 5 december 2011 schriftelijk aan het CBP verstrekt.

Het CBP heeft op 12 januari 2012 het Rapport voorlopige bevindingen vastgesteld. Het CBP heeft Vodafone bij brief van 13 januari 2012 in de gelegenheid gesteld om haar zienswijze op het Rapport voorlopige bevindingen naar voren te brengen. Vodafone heeft bij e-mail van 5 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 7 februari 2012 twee weken uitstel verleend, tot en met 24 februari 2012. Bij e-mail van 21 februari 2012 heeft Vodafone een tweede uitstel gevraagd in verband met [VERTROUWELIJK], tot 2 maart 2012. Bij brief van 22 februari 2012 heeft het CBP het gevraagde uitstel verleend. Vodafone heeft haar zienswijze op 2 maart 2012 schriftelijk ingebracht.

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

In de brief bij de zienswijze heeft Vodafone verzocht om in overleg te treden met het CBP over feitelijke, technische misvattingen in het rapport. Vodafone heeft dit verzoek om overleg om onduidelijkheden en misverstanden weg te nemen, herhaald bij e-mail van 2 april 2012. Bij brief van 3 april 2012 heeft het CBP dit verzoek afgewezen.

Op 11 juni 2012 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en [VERTROUWELIJK] en de [VERTROUWELIJK] van Vodafone over het onderzoek. Daarbij heeft het CBP mondeling aanvullende vragen gesteld over de

---

<sup>16</sup> Van de tijdens het onderzoek ter plaatse opgestelde en geprinte/gekopieerde bescheiden is een kopie aan Vodafone verstrekt.



zienswijze. Bij e-mail van 2 juli 2012 heeft het CBP deze vragen herhaald. Vodafone heeft de gevraagde toelichting op 10 juli 2012 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 Agentschap Telecom respectievelijk OPTA.

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

Het CBP heeft Vodafone bij brief van 21 augustus 2012 (door Vodafone ontvangen op 27 augustus 2012) in de gelegenheid gesteld om haar zienswijze op het Conceptrapport definitieve bevindingen naar voren te brengen. Vodafone heeft bij brief van 14 september 2012 verzocht om uitstel van de termijn voor het geven van een zienswijze tot en met 30 oktober 2012. Het CBP heeft bij e-mail van 19 september 2012 (per brief bevestigd op 20 september 2012) het door Vodafone gevraagde uitstel verleend. Vodafone heeft haar zienswijze op 30 oktober 2012 schriftelijk ingebracht.

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

Vodafone heeft bij (fax)brief van 31 december 2012, aangevuld in een telefoongesprek op 8 januari 2013, verzocht om uitstel van de termijn voor het geven van een reactie op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden tot en met 15 februari 2013 (eerst: 28 februari 2013).

Op 2, 8, 9 en 11 januari 2013 heeft telefonisch en per e-mail contact plaatsgevonden tussen (de advocaat-gemachtigde van) Vodafone en medewerkers van het CBP over de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden/het onderzoek.

Het CBP heeft bij brief van 9 januari 2013 uitstel verleend tot en met 21 februari 2013.

Op 14 januari 2013 heeft telefonisch overleg plaatsgevonden tussen medewerkers van het CBP en de advocaat-gemachtigde en medewerkers van Vodafone, om vragen van Vodafone over de vordering van het CBP te beantwoorden.

Vodafone heeft bij brief van 21 februari 2013 gereageerd op de vordering om inlichtingen en inzage in zakelijke stukken en bescheiden. Vodafone heeft daarbij aangegeven de gevorderde bescheiden niet aan het CBP te kunnen verstrekken in verband met een bevoegdheidsgebrek in de vordering van 20 december 2012.

Op 6 maart 2013 heeft telefonisch en per e-mail contact plaatsgevonden tussen (de advocaat-gemachtigde van) Vodafone en een medewerker van het CBP over de vordering van 20 december 2012/het onderzoek.

Op 7 maart 2013 heeft het CBP een herstellvordering aan Vodafone gezonden. Vodafone heeft bij brief van 8 maart 2013 de gevorderde bescheiden aan het CBP verstrekt.

Op 10 en 11 april 2013 heeft telefonisch overleg plaatsgevonden tussen de advocaat-gemachtigde van Vodafone en een medewerker van het CBP over 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 Agentschap Telecom.

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

### **Zienswijze 1 van Vodafone van 2 maart 2012 op het Rapport voorlopige bevindingen**

In haar zienswijze van 2 maart 2012 op het Rapport voorlopige bevindingen (hierna: zienswijze 1) brengt Vodafone, samengevat weergegeven, naar voren dat Vodafone in overeenstemming met de Wbp handelt. Zij verzamelt persoonsgegevens uitsluitend voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat daarbij om facturering in brede zin, waaronder verkeersbeheer, beveiliging en het behandelen van vragen en klachten van klanten. De verwerkingen zijn ook noodzakelijk voor de uitvoering van de overeenkomsten van Vodafone met haar klanten en het optimaliseren van haar dienstverlening. Deze doeleinden zijn ook in de melding van Vodafone bij het CBP opgenomen.

Het CBP miskent dat Vodafone verkeersgegevens (waar het in dit geval om gaat) op de voet van artikel 11.5 van de Tw voor het brede factureringsdoeleinde mag verwerken. Ook los daarvan heeft Vodafone voor elke verwerking van persoonsgegevens een grondslag in de zin van artikel 8, onder b, c en f, van de Wbp.

Ofschoon Vodafones huidige melding aan de eisen van de Wbp voldoet, is zij bereid haar melding onverplicht uit te breiden. Zij legt als bijlage bij de zienswijze een voorstel tot aanpassing aan het CBP voor.

Ofschoon Vodafone haar abonnees voldoende informatie verstrekt, is zij bereid haar Privacy Statement eveneens onverplicht aan te passen. Zij legt als bijlage een voorstel tot aanpassing aan het CBP voor.

Ook overigens heeft Vodafone in het onderzoek van het CBP aanleiding gezien om een aantal zaken op het gebied van privacy verder aan te scherpen (bijvoorbeeld het verkorten van de bewaartermijnen).

Het Rapport voorlopige bevindingen bevat volgens Vodafone een aantal feitelijke/wezenlijke misvattingen. Daarbij wijst Vodafone erop dat de fabrikant van de apparatuur waar het CBP op doelt bij de verwijzing naar een technisch systeem op grond waarvan verwerking van gegevens minder ingrijpend zou kunnen plaatsvinden, heeft verklaard dat een dergelijke aanpassing geen lichtere 'inbreuk' oplevert, maar wel een significante verslechtering van de dienstverlening zal betekenen.

Vodafone meent dat het CBP technische versimpelingen, een onjuist OSI-model en een inaccurate envelop-metafoor hanteert, wat tot onjuiste juridische kwalificaties leidt.

Het Rapport voorlopige bevindingen bevat volgens Vodafone verder zodanige onjuistheden over de werkwijze van Vodafone en suggestieve bewoordingen dat publicatie in de huidige vorm onrechtmatig is.

Vodafone nodigt het CBP uit om in een dialoog alle misvattingen weg te nemen.<sup>17</sup>

In **bijlage IV** bij dit rapport is de zakelijke inhoud van de zienswijze 1 van Vodafone opgenomen per onderdeel (met de toevoeging '**Zienswijze 1 Vodafone**'), met de reactie daarop van het CBP (zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd en aangevuld met in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van dat Conceptrapport definitieve bevindingen). Deze bijlage vormt een integraal onderdeel van dit rapport.

#### **Zienswijze 2 van Vodafone van 30 oktober 2012 op het Conceptrapport definitieve bevindingen**

In haar zienswijze 2 van 30 oktober 2012 op het Conceptrapport definitieve bevindingen (daaronder in dit geval mede begrepen de daaropvolgende correspondentie als beschreven onder het kopje 'Verloop onderzoek', p. 10 e.v. van dit rapport) brengt Vodafone, samengevat weergegeven, naar voren dat het onderzoek onzorgvuldig is en daarom moet worden beëindigd. Vodafone noemt (kort gezegd) de navolgende redenen.

Vodafone stelt dat er onduidelijkheid is (geweest) omtrent de reikwijdte, het onderwerp van onderzoek en de onderzoeksvragen en dat de reikwijdte van het onderzoek is aangepast. Vodafone meent dat zij daardoor is gedwongen om mee te werken aan haar eigen veroordeling.

Vodafone meent dat het CBP niet een Conceptrapport definitieve bevindingen aan haar had mogen voorleggen voor een tweede zienswijze, laat staan dat het na de zienswijze 1 extra overtredingen had mogen constateren. Dit bijvoorbeeld omdat mogelijk een (punitieve) sanctie kan worden opgelegd.

Volgens Vodafone bevat het Conceptrapport definitieve bevindingen ondanks de informatie en antwoorden die het CBP van Vodafone heeft gekregen nog steeds feitelijke onjuist- en onzorgvuldigheden. De rechtszekerheid - en artikel 6 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) - vereist daarom dat het onderzoek moet worden gesloten.

Vodafone geeft aan dat het in strijd met het fair play-beginsel, onzorgvuldig en in strijd met het zelfincriminatieverbod is dat het CBP niet in overleg wil treden met haar over de melding, het Privacy Statement, het terugbrengen van bewaartermijnen en het herhaaldelijke aanbod van Vodafone om in gezamenlijk overleg te overzien hoe eventuele overtredingen zo snel en zo effectief mogelijk kunnen worden beëindigd.

---

<sup>17</sup> Zienswijze Vodafone van 2 maart 2012, p. 9-10 (doorgenummerde pagina's op de faxbrief).

In haar zienswijze 2 wijst Vodafone erop dat het CBP ten onrechte kwalificaties geeft over de rechtmatigheid van het gebruik van 'data-analyse technieken' onder nieuwe regelgeving (artikel 7.4a en artikel 11.2a van de Tw (nieuw)).

Volgens Vodafone heeft het CBP onvoldoende gemotiveerd waarom er ten aanzien van bepaalde data-analyse technieken alternatieve, voor de betrokken eindgebruikers vermeend lichtere maatregelen kunnen worden gebruikt (ten onrechte is ook niet in kaart gebracht wat de gevolgen, bijvoorbeeld voor de netwerkindegriteit en -stabiliteit, zouden zijn van zulke alternatieven). Ook zou het CBP tegenbewijs van Vodafone niet hebben meegenomen.

Vodafone merkt op dat het CBP zich ten onrechte op detailniveau inlaat met de dagelijkse bedrijfsvoering van Vodafone, door niet of nauwelijks gemotiveerde voorstellen.

Dat het CBP blijft vasthouden aan onjuiste, suggestieve indelingen en beschrijvingen, in combinatie met het feit dat het CBP niet in overleg wil treden met Vodafone en de in de ogen van Vodafone voor het CBP voordelige interpretatie van de wettelijke regels wijst volgens Vodafone op strijd met het verbod van vooringenomenheid.

Vodafone geeft in haar zienswijze 2 aan dat het Conceptrapport definitieve bevindingen volgens haar inconsistent is van opzet en structuur.

Vodafone meent dat zij op geen enkele wijze de Wbp of de Tw heeft overtreden of overtreedt. Er bestaan ook geen andere, minder ingrijpende middelen om hetzelfde resultaat te bereiken.

In **bijlage V** bij dit rapport is de zakelijke inhoud van de zienswijze 2 van Vodafone opgenomen per onderdeel (met de toevoeging '**Zienswijze 2 Vodafone**'), 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

Vodafone, gevestigd te Maastricht, is opgericht op 10 december 1991 en ingeschreven bij de Kamer van Koophandel onder nummer 14052264. De doelomschrijving van Vodafone is: *“Het exploiteren en verder ontwikkelen van een mobiel telecommunicatienetwerk gebaseerd op gsm en/of dcs 1800 en/of andere technologieën en het verlenen van telecommunicatiediensten.”*

Vodafone is geregistreerd bij de ACM als aanbieder van een openbare elektronische communicatiedienst en -netwerk.<sup>18</sup>

Vodafone had in 2011 een marktaandeel op de markt voor mobiele telefonie in Nederland van ongeveer 26%<sup>19</sup>, en 25 tot 30% per eind 2012<sup>20</sup> (5,1 miljoen klanten medio 2011<sup>21</sup>, 5,3 miljoen klanten per 31 maart 2012<sup>22</sup>). Niet alle Vodafone-klanten hebben ook toegang tot mobiel internet. Uit de cijfers van Vodafone blijkt dat het aantal smartphones van abonnees op haar netwerk in 2011-2012 met 50% is toegenomen, bij prepaid abonnees met 90% ten opzichte van het boekjaar daarvoor.<sup>23</sup> Uit de Openbare rapportage mobiel Q4 2012 blijkt dat ongeveer 46,4% van de Nederlandse mobiele telefonieaansluitingen eind 2012 toegang had tot mobiel internet.<sup>24</sup> Volgens recente gegevens van Telecompaper heeft meer dan 60% van de Vodafone abonnees in Nederland inmiddels mobiel internet.<sup>25</sup> Omgerekend voor Vodafone betreft het sinds eind 2012 bijna 3,2 miljoen abonnees.

---

<sup>18</sup> URL:

<https://www.acm.nl/nl/onderwerpen/telecommunicatie/registraties/geregistreerde-ondernemingen/resultaat/?query=vodafone+libertel+b.v.&categorie=&plaats=> (URL laatst bezocht op 29 mei 2013).

<sup>19</sup> Volgens gegevens uit de halfjaarlijkse Marktrapportage Elektronische Communicatie van TNO had Vodafone aan het eind van het tweede kwartaal van 2011 5,1 miljoen mobiele aansluitingen. TNO-rapport. Marktrapportage Elektronische Communicatie December 2011, Delft: TNO 2011, p. 15. URL: <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/01/18/marktrapportage-elektronische-communicatie.html>. De betreffende marktrapportage bevat geen cijfers over het percentage Vodafone klanten dat gebruik maakt van mobiele datadiensten. Op basis van het aantal aansluitingen voor mobiele telefonie lag het marktaandeel van Vodafone volgens het jaarverslag van OPTA aan het eind van het tweede kwartaal van 2012 tussen 25 en 30 procent. OPTA jaarverslag 2012, p. 10. URL: <http://optajaarverslag2012.acm.nl> (URL's laatst bezocht op 29 mei 2013).

<sup>20</sup> Openbare rapportage mobiel Q4 2012, p. 2.

<sup>21</sup> TNO-rapport. Marktrapportage Elektronische Communicatie December 2011, Delft: TNO 2011, p. 15: *“Vodafone zag het aantal aansluitingen stijgen met 4,2 % naar 5,1 miljoen.”*

<sup>22</sup> ‘Jaarcijfers Vodafone Nederland: groei ondanks krimpende telecommarkt’, *Persbericht Vodafone* 22 mei 2012. URL: [http://over.vodafone.nl/nieuwscentrum/nieuws/jaarcijfers-vodafone-nederland-groei-ondanks-krimpende-telecommarkt?from\\_search](http://over.vodafone.nl/nieuwscentrum/nieuws/jaarcijfers-vodafone-nederland-groei-ondanks-krimpende-telecommarkt?from_search) (URL laatst bezocht op 29 mei 2013).

<sup>23</sup> Idem.

<sup>24</sup> Openbare rapportage mobiel Q4 2012, p. 1. Zie ook OPTA jaarverslag 2012, p. 7: *“Ruim 45 procent van de aansluitingen voor mobiele telefoons wordt ook gebruikt voor internet.”*

<sup>25</sup> ‘Consumenten kopen handset in winkel, bestellen sim online’, *Telecompaper* 11 juli 2012.

Volgens cijfers van Vodafone maakt [VERTROUWELIJK] van het aantal prepaid abonnees van Vodafone gebruik van mobiel internet. Vodafone heeft NAW-gegevens en/of e-mailadressen van [VERTROUWELIJK] van deze prepaid abonnees.<sup>26</sup>

Vodafone heeft de verwerking van persoonsgegevens, voor zover voor dit onderzoek van belang, op 13 maart 2008 gemeld bij het CBP onder nummer m1040032 (versienummer 2.0). In de melding zijn, voor zover voor dit onderzoek van belang, als doelen van verwerking genoemd:

Verwerking van gegevens van gebruik. en pot. gebruikers van het Vodafone netwerk (m1040032)

|                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Het sluiten en uitvoeren van de overeenkomst die het gevolg is van de voornoemde aansluiting [dat wil zeggen: spraak en data, toevoeging door het CBP]           |
| Het nakomen van de contractuele verplichtingen uit de overeenkomst                                                                                               |
| Het opstellen van profielen van (potentiële) Vodafone gebruikers ten behoeve van het uitbreiden en optimaliseren van omzet, klantenbestand en producten/diensten |
| Het voorkomen van fraude en misbruik en het bevorderen van de continuïteit en beveiliging van de Vodafone organisatie en het Vodafone netwerk                    |
| Kwaliteits- en marktonderzoeken en training/opleiding van eigen personeel <sup>27</sup>                                                                          |

Vodafone heeft geen andere melding(en) gedaan die betrekking hebben op de verwerking van gegevens over en uit het mobiele dataverkeer bij de inzet van data-analyse technieken. Vodafone heeft geen eigen functionaris voor de gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.<sup>28</sup>

Vodafone heeft verklaard dat de melding onder nummer m1040032 geen betrekking heeft op het gebruik van gegevens in dan wel afkomstig uit packet inspection voor marketingdoeleinden.<sup>29</sup>

### **Voorgenomen maatregelen**

Vodafone heeft in haar zienswijze 1 naar voren gebracht dat ze onverplicht bereid is de melding uit te breiden. Een voorstel tot aanpassing is als bijlage bij de zienswijze gevoegd.<sup>30</sup>

In het voorstel tot aanpassing wordt het doel van verwerking 'Het sluiten en uitvoeren van de overeenkomst die het gevolg is van de voornoemde

<sup>26</sup> Reactie Vodafone op verzoek om inlichtingen van 11 april 2012.

<sup>27</sup> In de melding zijn, voor zover voor dit onderzoek van belang, als categorie(ën) (soorten) van betrokkenen en gegevens genoemd: 'Gebruikers en potentiële gebruikers van het Vodafone netwerk c.q de Vodafone diensten' respectievelijk 'Contractgegevens (gebruikersnaam, mobiel nr en andere personalia)', 'Servicegegevens', 'Abonnementsgegevens', 'Aansluitgegevens', 'Betalingsgegevens', 'Interesse- en voorkeursgebieden', 'Nota/debiteuren gegevens', 'Verkeersgegevens' en 'Logging Customer Services'.

<sup>28</sup> Zie Register van Functionarissen voor de Gegevensbescherming. URL: [http://www.cbpreweb.nl/Pages/ind\\_reg\\_fggreg.aspx](http://www.cbpreweb.nl/Pages/ind_reg_fggreg.aspx) (URL laatst bezocht op 29 mei 2013).

<sup>29</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 9: "Vodafone gebruikt gegevens in dan wel afkomstig uit packet inspection niet voor marketing doeleinden."

<sup>30</sup> Zienswijze 1 Vodafone, p. 9, 17 en 42 (doorgenummerde pagina's op de faxbrief) en bijlage 6 bij deze zienswijze.

aansluiting' uitgebreid met de zinsnede "(...) inclusief het leveren van producten en diensten, het factureren waaronder begrepen het factureren van MMS-verkeer en debiteurenadministratie alsmede verkeer- en netwerkmanagement, waaronder begrepen transporteren van het verkeer van prepaidklanten naar opwaardeersites en videocompressie, om het gebruik van het netwerk te kunnen analyseren, de continuïteit, beveiliging en integriteit van het netwerk te waarborgen en te bevorderen, (gevolgen van) congestie te beperken en fraude en hoog verbruik te detecteren (onder andere voor bill-shock preventie)." Vodafone stelt daarnaast voor om 'facturering en debiteurenadministratie, verkeersbeheer' als doel waarvoor de gegevens zijn/worden verzameld (eveneens) te vervangen door de hierboven weergegeven uitgebreide tekst. Vodafone stelt verder voor om het doel 'Klachtoplossing, afhandeling verzoeken om inlichtingen van klanten/gebruikers en berechting en beslissing van geschillen' toe te voegen als doel van verwerking én als doel waarvoor de gegevens zijn/worden verzameld (dit laatste ter vervanging van 'berechting en beslechting van geschillen').<sup>31</sup>

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

Vodafone maakt voor wat betreft netwerkopbouw een onderscheid (op technologie): 2G voor voice en GPRS-dataverkeer en 3G voor voice en UMTS-dataverkeer. Deze staan in verbinding met elkaar.<sup>32</sup> Mobiele apparaten, zoals smartphones gebruiken zowel het voice- als dataverkeer-gedeelte van het netwerk, al naar gelang de gebruikte dienst (spraak of data).

Het mobiele netwerk is daarnaast verder te verdelen in een radiotoegangsnetwerk- en een core-netwerkgedeelte (zie **bijlage I**).

Het mobiele netwerk van Vodafone vervoert niet alleen spraak- en dataverkeer, maar ook signaleringsverkeer (kleine berichten die nodig zijn om de verbinding op te bouwen, in stand te houden en te verbreken). Spraak-, data- en signaleringsverkeer maken gebruik van dezelfde radioweg (toegang tot het radiotoegangsnetwerk). Elk onderdeel van het mobiele netwerk heeft een maximum capaciteit (zie ook het kopje 'Aanleiding onderzoek', p. 6 e.v. van dit rapport).

Het 3G-gedeelte van het mobiele radiotoegangsnetwerk bestaat uit *Base Stations* ('Node B'; antenne radiomast) en *Radio Network Controllers* (RNC; netwerkelement waar de gegevens worden versleuteld voordat deze worden verzonden naar en van het mobiele apparaat). In het core-netwerk bevinden zich databases<sup>33</sup> en netwerkelementen die nodig zijn voor het leveren van diensten, zoals de *Serving GPRS Support Node* (SGSN) die de binnenkomende radiosignalen omzet in GTP-controle plane (GTP-C; oftewel, het signaleringskanaal) en GTP-user plane (GTP-U; oftewel, het

<sup>31</sup> Idem, bijlage 6.

<sup>32</sup> 'Vodafone gaat 2G- en 3G-netwerken scheiden', *Webwereld* 2 juli 2012. URL: <http://webwereld.nl/mobility/57295-vodafone-gaat-2g--en-3g-netwerken-scheiden> (URL laatst bezocht op 29 mei 2013).

<sup>33</sup> Bijvoorbeeld het *Home Location Register* (databank waarin onder meer het MSISDN, het IMSI en informatie over de (prepaid of postpaid) datadiensten waar de abonnee op is geabonneerd, zijn opgeslagen) en het *Visitor Location Register* (databank waarin de exacte locatie van gebruikers van het mobiele netwerk wordt bijgehouden).

dataverkeerskanaal) en de *Gateway GPRS Support Node* (GGSN) die het dataverkeer doorgeeft aan externe netwerken, zoals het internet (zie ook **bijlage III**, de verklarende woordenlijst bij dit rapport).

Vodafone maakt gebruik van data-analyse technieken op het dataverkeer (inclusief signaleringsverkeer) in haar mobiele netwerk<sup>34</sup>, ten behoeve van de dienstverlening aan haar klanten.<sup>35</sup> [VERTROUWELIJK]

Met gebruikmaking van de data-analyse apparatuur inspecteert en analyseert Vodafone, kort gezegd, datapakketten/datapakketgegevens. Daartoe worden datapakketten door/langs een filter met inspectieregels geleid. Data-analyse apparaten verwerken niet meer dan dat waarvoor ze zijn ingesteld. [VERTROUWELIJK]

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

Vodafone verkrijgt via de data-analyse apparatuur gegevens over en (in een enkel geval) uit<sup>36</sup> het dataverkeer van potentieel alle<sup>37</sup> ongeveer 3,2 miljoen Vodafone abonnees met een (prepaid of postpaid) data abonnement en van de gebruikers van haar dataverkeersdiensten.

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

---

<sup>34</sup> Zie Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 2-3 en Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1: “*Vodafone analyseert verkeersgegevens van haar klanten voor meerdere doeleinden. (...)*”

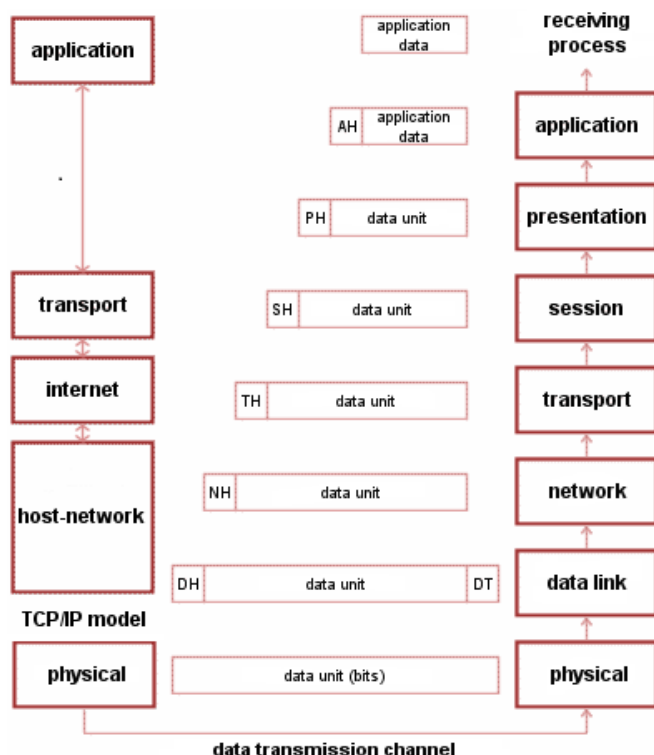
<sup>35</sup> Zienswijze 1 Vodafone, p. 10 (doorgenummerde pagina’s op de faxbrief).

<sup>36</sup> Zie o.a. Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 2: “*(...) de inhoud van de communicatie van klanten wordt niet geïnspecteerd, afgeluisterd of op andere wijze ingezien. Hierop bestaan slechts twee legitieme uitzonderingen: 1) als Vodafone moet voldoen aan haar wettelijke verplichting om gevorderde gegevens aan politie en justitie te verstrekken en 2) als de klant Vodafone hiervoor uitdrukkelijke toestemming heeft gegeven.*”

<sup>37</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 2-3.



AFBEELDING 1 Opbouw packets volgens TCP-IP en OSI-model<sup>38</sup>



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

Inhoud van het verkeer/payload wordt in dit rapport gedefinieerd als gegevens 'uit' het dataverkeer.

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

## 2.3 Overzicht doeleinden

Vodafone verklaart dat er (limitatief) drie doeleinden zijn voor de toepassing van data-analyse technieken in haar mobiele netwerk.

<sup>38</sup> Bron: [http://www2.themanualpage.org/networks/networks\\_osi2.php3](http://www2.themanualpage.org/networks/networks_osi2.php3). Zie ook Zienswijze 1 Vodafone, p. 16 (doorgenummerde pagina's op de faxbrief).

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. Verkeersbeheer en facturering.</p> <p><b>Verkeersbeheer</b><sup>39</sup>, waaronder het detecteren en oplossen van problemen in het netwerk<sup>40</sup> en om de gevolgen van congestie te beperken.<sup>41</sup> Het monitoren van het verkeer om het gebruik van het netwerk en de gebruikservaring van Vodafone-klanten te optimaliseren (video optimalisatie)<sup>42</sup> en netwerkplanning (<i>forecasting</i>/dimensionering).<sup>43</sup></p> <p><b>Facturering.</b><sup>44</sup> Bijvoorbeeld het detecteren van applicaties (apps) die volgens de Dienstvoorwaarden Vodafone BloX niet mogen worden gebruikt<sup>45</sup> (om peer-to-peer misbruik en excessieve overschrijdingen van haar <i>Fair Use Policy</i> te voorkomen)<sup>46</sup> en om klanten te behoeden voor de zogenaamde 'billshock' en hen tijdig te (kunnen) waarschuwen dat zij hun data <i>roaming</i><sup>47</sup> cap van EUR 50 bijna hebben bereikt.<sup>48</sup> Ook de facturering van MMS-verkeer<sup>49</sup> en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites.<sup>50</sup></p> |
| <p>2. <b>Beveiliging.</b> Voor het gebruik van spam- en virusfilters en het detecteren van botnets in het netwerk<sup>51</sup>, maar ook tegen andere vormen van <i>malware</i> zoals <i>trojans</i> en inbraakpogingen.<sup>52</sup> Om de integriteit en veiligheid van haar netwerk(en) en diensten te waarborgen.<sup>53</sup></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>3. <b>Behandeling van verzoeken om inlichtingen van klanten.</b><sup>54</sup> Om klachten en problemen van klanten op te lossen.<sup>55</sup> Anders gezegd: het met uitdrukkelijke toestemming van een abonnee onderzoeken van zijn of haar dataverkeer in verband met het onderzoek naar een klacht.<sup>56</sup></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Hierna worden achtereenvolgens beschreven de gegevensverwerkingen voor de hierboven genoemde doeleinden én het gebruik van rapportages voor het vaststellen van de *business strategie* van Vodafone (zie paragraaf 2.8, p. 47 van dit rapport).

<sup>39</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1.

<sup>40</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3

<sup>41</sup> Brief Vodafone van 21 november 2011, p. 5.

<sup>42</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>43</sup> Idem en verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011.

<sup>44</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1.

<sup>45</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 2-3 en Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1-2.

<sup>46</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>47</sup> Te weten: de situatie waarin een bepaalde telecommunicatiedienst wordt voortgezet hoewel de gebruiker zich niet in het netwerk bevindt waarin deze geregistreerd staat (dat wil zeggen: daar waar hij klant is). Dankzij roaming kan hij met zijn mobiele telefonie abonnement ook in het buitenland bellen/gebruik maken van mobiel internet. Een toelichting op roaming is te lezen op: URL: <http://nl.wikipedia.org/wiki/Roaming> (URL laatst bezocht op 11 mei 2013).

<sup>48</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>49</sup> Idem, p. 8.

<sup>50</sup> Idem.

<sup>51</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1.

<sup>52</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>53</sup> Brief Vodafone van 21 november 2011, p. 5.

<sup>54</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 2. Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1-2.

<sup>55</sup> Brief Vodafone van 21 november 2011, p. 5.

<sup>56</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1.

## 2.4 Verkeersbeheer

Als eerste verzamel- en verwerkingsdoeleinde van gegevens noemt Vodafone verkeersbeheer en facturering, waaronder - samengevat weergegeven - netwerkplanning (forecasting/dimensionering), netwerkmonitoring (het detecteren en oplossen van problemen in het netwerk), video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites.

### Aanleiding toepassing data-analyse technieken netwerkplanning

Vodafone verklaart dat het verkrijgen van gegevens met betrekking tot het mobiele dataverkeer door middel van data-analyse technieken noodzakelijk is voor (onder andere) netwerkplanning: “(...) *gelet op het toegenomen gebruik van smart phones en mobiel internet - [is, toevoeging door het CBP] het gebruik van deze technieken noodzakelijk (...) om een normaal gebruik van haar netwerken en diensten blijvend te kunnen waarborgen.*”<sup>57</sup>

Vodafone licht toe: “*Er zijn meerdere redenen aan te voeren om de noodzakelijkheid van een kwalitatieve analyse te onderbouwen. De belangrijkste reden is dat het gebruik van het netwerk regelmatig wijzigt in verband met het gebruik van nieuwe toestellen, zoals smartphones. Het verkeersprofiel, en dus ook de netwerkbelasting, wijzigt steeds vaker. Het aantal gebruikers van een smartphone wordt bijvoorbeeld steeds groter en er wordt steeds meer gebruik gemaakt van applicaties die grote invloed hebben op beide kanalen.*(...) Omdat bestaande applicaties in populariteit kunnen dalen en er veel nieuwe applicaties worden aangeboden is het belangrijk om dit goed te blijven monitoren”, (onderstreping toegevoegd door het CBP).<sup>58</sup>

Vodafone licht in haar zienswijze 1 nader toe over waarom verkeersbeheer een vereiste is om het netwerk goed te laten (blijven) functioneren, gezien de explosieve toename van het datagebruik als gevolg van smartphones, tablets etc.: “*Dataverkeer over mobiele netwerken nam de afgelopen 4 jaar met een factor 2-3 per jaar toe. Het totale mobiele dataverkeer in 2011 was een factor 8 van het mondiale dataverkeer (vast en mobiel) in 2000. (...) Smartphones vertegenwoordigen 82% van het dataverkeer. Tablets genereren 3,4 keer meer data dan een smartphone. [VERTROUWELIJK] In de komende vier jaar zal het mobiele dataverkeer met een factor 18 groeien. (...) Netwerkbeheer en -forecasting betekent, gelet op deze cijfers, kortom dat dagelijks alle zeilen moeten worden bijgezet om het netwerk te laten blijven functioneren (...).*”<sup>59</sup>

Mobiele apparaten, zoals smartphones (en daarop geïnstalleerde/gebruikte apps), maken ander(s) gebruik van het mobiele netwerk dan reguliere toestellen. Ze maken veel vaker contact met het internet, en gebruiken daarvoor telkens het signaleringskanaal (en het radiotoegangsnetwerk).<sup>60</sup> Zo verbreken smartphones veelvuldig de verbinding om de batterij te sparen. Er zijn apps die vaak weer verbinding (doen) zoeken met het netwerk, om gegevens te verversen door data van de server af te halen of te checken of er updates beschikbaar zijn. Dit fenomeen wordt

<sup>57</sup> Brief Vodafone van 21 november 2011, p. 5.

<sup>58</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 2-3.

<sup>59</sup> Zienswijze 1 Vodafone, p. 17-18 (doorgenummerde pagina's op de faxbrief).

<sup>60</sup> Vgl. o.a. Chris Foresman, 'How smartphones are bogging down some wireless carriers', *Ars technica* 22 februari 2010. URL: <http://arstechnica.com/gadgets/news/2010/02/how-smartphones-are-bogging-down-some-wireless-carriers.ars> (URL laatst bezocht op 29 mei 2013).

wel 'chatty apps' genoemd en leidt tot een significante toename van het signaleringsverkeer. Als het radiotoegangsnetwerk crasht als gevolg van teveel signaleringen in het GPRS- of UMTS-gedeelte kan er ook niet meer worden gebeld.

Vodafone schrijft in dat verband: *"Voorbeelden zijn Facebook en Twitter die veel statuscontroles uitvoeren die een extra belasting op het netwerk met zich mee brengen, en dus een ander verkeersprofiel opleveren."*<sup>61</sup> Vodafone voegt daar in haar zienswijze 1 aan toe: *"Vodafone moet de oorzaak van de druk op het signaleringskanaal in kaart brengen om deze vervolgens te kunnen managen. (...) hierbij gaat het niet om 'de populariteit' of iets dergelijks van de verschillende toestellen en/of apps te controleren, maar de mate van netwerkbelasting. [VERTROUWELIJK] (...) Nieuwe apps komen dagelijks uit, en elke app heeft een eigen belasting op het signaleringskanaal (een eigen 'signaleringsoutput'); [VERTROUWELIJK]. Al deze ontwikkelingen - de verschillen tussen smartphones, én de impact van de grote hoeveelheid apps - illustreren de zeer dynamische (lees: zeer wisselende) belasting van het mobiele netwerk. Technieken om dat in kaart te brengen zijn onontbeerlijk in het kader van verkeersbeheer/tegengaan van congestie", (onderstreping toegevoegd door het CBP).*<sup>62</sup>

In haar zienswijze 1 vult Vodafone aan dat het noodzakelijk voor haar is om op individueel klantniveau gegevens te verwerken om valide, bruikbare informatie te krijgen over de netwerkbelasting als gevolg van de toename van het gebruik van allerlei websites en apps (ten behoeve van netwerkplanning en -beheer).<sup>63</sup> Vodafone licht (verder) toe: *"[VERTROUWELIJK],"* (onderstreping door Vodafone).<sup>64</sup>

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

In haar reactie op een verzoek om inlichtingen over de vraag of de netwerkbelasting die smartphones en apps veroorzaken ook op andere manieren kan worden gemeten, licht Vodafone toe: *"[VERTROUWELIJK]."*<sup>65</sup>

Volgens Vodafone kan ook niet worden volstaan met steekproefsgewijze controle: *"[VERTROUWELIJK]"*

Vodafone heeft verklaard de verhouding tussen de capaciteit in haar netwerk voor enerzijds data- en anderzijds signaleringsverkeer (gedeeltelijk) naar behoefte te kunnen aanpassen/veranderen.<sup>66</sup>

Het CBP heeft er (weliswaar) kennis van genomen dat er naast het uitbreiden van de (signalerings-)capaciteit in het mobiele netwerk ook andere mogelijkheden, en initiatieven bestaan om de druk op het signaleringskanaal te verminderen. Zo hebben volgens berichtgeving in de media grote mobiele aanbieders zoals France Telecom, Deutsche Telekom en Telefónica (Spanje) medio 2011 aangekondigd in overleg te

<sup>61</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 3.

<sup>62</sup> Zienswijze 1 Vodafone, p. 19 (doorgenummerde pagina's op de faxbrief).

<sup>63</sup> Idem, p. 37.

<sup>64</sup> Idem, p. 33.

<sup>65</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 3.

<sup>66</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011.

(willen) gaan met makers van besturingssystemen van smartphones en app-ontwikkelaars om de gebruikte software anders in te richten, op een manier die netwerkvriendelijker is.<sup>67</sup> De GSM Association, een wereldwijd samenwerkingsverband in de telecomindustrie, heeft in februari 2012 de eerste van een serie activiteiten aangekondigd, bedoeld om netwerkaanbieders te helpen om te gaan met het grotere aantal signaleringen als gevolg van smartphones en apps, te weten: 'Guidelines for Creating More Efficient Mobile Applications' (een developer's guide) en de 'Smarter Apps Challenge' (een competitie om de ontwikkeling van netwerkvriendelijkere apps te stimuleren).<sup>68</sup> Ter relativering van het belang en de mogelijkheden van zulke initiatieven wijst Vodafone er in haar zienswijzen (evenwel op dat ofschoon zij ook dit soort initiatieven ontplooit met fabrikanten van toestellen (te weten: om de gebruikte software anders in te richten, op een manier die netwerkvriendelijker is) de door het CBP aangehaalde initiatieven tot nu toe niet hebben geleid tot concrete oplossingen.<sup>69</sup>

Het CBP stelt verder vast dat het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, (de gevolgen van) de toename van het datavolume relativeert in de (concept) netneutraliteitsrichtsnoeren, met de volgende zinsneden: *"One should, however, refrain from drawing hasty conclusions from mobile data growth forecasts, which may often be exaggerated and may be compensated for, to a certain extent, by 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."*<sup>70</sup> Volgens Vodafone ziet dit rapport niet op data-analyse technieken, maar gaat het over netneutraliteit en is het geschreven vanuit een economische, en niet een technische achtergrond.<sup>71</sup>

<sup>67</sup> Zie Michelle Donegan, 'Operators Urge Action Against Chatty Apps' (Verslag over de Open Mobile Summit), *Light Reading Mobile* 9 juni 2011. URL: [http://www.lightreading.com/document.asp?doc\\_id=208775](http://www.lightreading.com/document.asp?doc_id=208775) (URL laatst bezocht op 29 mei 2013).

<sup>68</sup> GSM Association, 'GSMA Announces New Initiatives Focusing On Creating More Efficient Mobile Applications', 27 februari 2012. URL: <http://www.gsma.com/newsroom/gsma-announces-new-initiatives-focusing-on-creating-more-efficient-mobile-applications/> (URL laatst bezocht op 29 mei 2013).

<sup>69</sup> Zienswijze 1 Vodafone, p. 18-19 (doorgenummerde pagina's op de faxbrief) en Zienswijze 2 Vodafone, p. 30.

<sup>70</sup> BoR (12) 131. BEREC Guidelines for quality of service in the scope of net neutrality, dated 26 November 2012, p. 17. URL: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/regulatory\\_best\\_practices/guidelines/?doc=1101](http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/?doc=1101). Zie ook BEREC Guidelines for Quality of Service in the scope of Net Neutrality. Draft for public consultation, dated 29 May 2012, p. 17. URL: [http://berec.europa.eu/files/news/bor\\_12\\_32\\_guidelines.pdf](http://berec.europa.eu/files/news/bor_12_32_guidelines.pdf) (URL's laatst bezocht op 29 mei 2013).

<sup>71</sup> Zienswijze 2 Vodafone, p. 24 en 30.

### Data-analyse apparatuur netwerkplanning

Vodafone gebruikt [VERTROUWELIJK] verschillende soorten data-analyse apparatuur (meetapparaten) ten behoeve van netwerkplanning. Het gaat om de [VERTROUWELIJK: apparatuur].<sup>72</sup>

#### [VERTROUWELIJK]

De [VERTROUWELIJK: apparatuur] wordt door Vodafone [VERTROUWELIJK] gebruikt voor netwerkplanning (forecasting/dimensionering), om op een geaggregeerd niveau inzicht te krijgen in het dataverbruik op het netwerk (bijvoorbeeld %VOIP, [VERTROUWELIJK]).<sup>73</sup> Dit om trends te kunnen volgen, [VERTROUWELIJK].<sup>74</sup> Uit de (product)documentatie en print-outs van het onderzoek ter plaatse volgt dat de data-analyse apparatuur in staat is om [VERTROUWELIJK] (zie **afbeelding 2 tot en 4** hieronder).<sup>75</sup> De apparatuur gebruikt [VERTROUWELIJK] om VOIP en peer-to-peer protocollen en diensten realtime te herkennen: [VERTROUWELIJK]

AFBEELDING 2 Grafische interface [VERTROUWELIJK]<sup>76</sup>  
[VERTROUWELIJK].

AFBEELDING 3 Grafische interface [VERTROUWELIJK]<sup>77</sup>

AFBEELDING 4 Grafische interface [VERTROUWELIJK]<sup>78</sup>

De [VERTROUWELIJK: apparatuur], zoals bij Vodafone in gebruik, heeft (aldus) als instelling dat deze gegevens verzamelt<sup>79</sup> vastlegt<sup>80</sup> en bewaart<sup>81</sup> over het bezoek van Vodafone abonnees aan websites en het gebruik van (een aantal) vooraf gedefinieerde apps en protocollen (voor zover zij die websites bezoeken of apps en protocollen gebruiken), zoals het verbruikte datavolume en de tijdseenheid, zoals [VERTROUWELIJK], web [hostname en VERTROUWELIJK]<sup>82</sup>,

---

<sup>72</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011 en Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 4.

<sup>73</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>74</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011.  
[VERTROUWELIJK]

<sup>75</sup> Zie o.a. [VERTROUWELIJK], p. 10 en Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 006, 007 en 009 tot en met 012.

<sup>76</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011,  
[VERTROUWELIJK: apparatuur] 010.

<sup>77</sup> Idem, [VERTROUWELIJK: apparatuur] 007.

<sup>78</sup> Idem, [VERTROUWELIJK: apparatuur] 006.

<sup>79</sup> [VERTROUWELIJK: apparatuur], p. 10-11 en Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 014 tot en met 017.

<sup>80</sup> Idem, p. 11 en Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011,  
[VERTROUWELIJK: apparatuur] 013 tot en met 017.

<sup>81</sup> Idem, p. 19 en Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011,  
[VERTROUWELIJK: apparatuur] 013 tot en met 017.

<sup>82</sup> Idem en [VERTROUWELIJK: apparatuur] 010, 016 (**afbeelding 2 en 5** in dit rapport) en 017 en 005. [VERTROUWELIJK]

VoIP [VERTRouwELIJK], *streaming*, [VERTRouwELIJK], *peer-to-peer* [VERTRouwELIJK].<sup>83</sup>

AFBEELDING 5 [VERTRouwELIJK]<sup>84</sup>  
[VERTRouwELIJK].

Technisch vindt de data-analyse door Vodafone als volgt plaats.

Data- en signaleringsverkeer packets van alle Vodafone abonnees worden *realtime* door/langs een filter met inspectieregels geleid. De gedetecteerde gegevens met betrekking tot het bezoek aan websites op hostname-niveau en het gebruik van de hierboven genoemde vooraf gedefinieerde apps en protocollen worden vervolgens geordend in [VERTRouwELIJK].<sup>85</sup>

AFBEELDING 6 [VERTRouwELIJK]<sup>86</sup>  
[VERTRouwELIJK].

Vodafone verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement (afhankelijk van de websites die zij bezoeken of apps en protocollen die zij gebruiken) enerzijds het [VERTRouwELIJK: identifiërs] en anderzijds de hostname (URL op hoofddomein) van de website/app<sup>87</sup> of het IP-adres van-naar met poortnummer/protocol<sup>88</sup> [VERTRouwELIJK], evenals aantallen bytes (volume) [VERTRouwELIJK]<sup>89</sup>, starttijd en eindtijd sessie/tijdsvenster.<sup>90</sup>

Vervolgens worden deze gegevens in ruwe vorm opgeslagen, waarna ze gedurende zeven dagen worden bewaard in een achterliggende database.<sup>91</sup> [VERTRouwELIJK]

Na één dag worden de gegevens op dagbasis geaggregeerd en opgeslagen in een tweede database die toegankelijk is via de grafische interface.<sup>92</sup> Uit de

---

<sup>83</sup> [VERTRouwELIJK] en Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTRouwELIJK: apparatuur] 005 (**afbeelding 7** in dit rapport).

<sup>84</sup> Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTRouwELIJK: apparatuur] 016.

<sup>85</sup> Zienswijze 1 Vodafone, p. 20 (doorgenummerde pagina's op de faxbrief). Zie ook Bijlage 1 bij Reactie Vodafone op vordering van 21 februari 2013 (verklaring van de leverancier): "[VERTRouwELIJK]."

<sup>86</sup> Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTRouwELIJK: apparatuur] 014 en 015.

<sup>87</sup> De categorieën [VERTRouwELIJK].

<sup>88</sup> De categorieën [VERTRouwELIJK]. E-mail Vodafone van 10 juli 2012: "(...) [VERTRouwELIJK] het gaat om het IP address van het netwerkelement en niet om het IP address van een specifieke Vodafone eindgebruiker. [VERTRouwELIJK]." De vraag of er sprake is van herleidbaarheid van zulke IP-adressen van netwerkelementen - op zichzelf - is niet door het CBP onderzocht. De inzet van data-analyse technieken valt buiten de scope van dit onderzoek voor zover het deze IP-adressen betreft.

<sup>89</sup> Zie o.a. de categorieën [VERTRouwELIJK].

<sup>90</sup> Zie o.a. de categorieën [VERTRouwELIJK].

<sup>91</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011. Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5.

<sup>92</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011 en Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTRouwELIJK]:

(product)documentatie bij de [VERTROUWELIJK: apparatuur] volgt, en Vodafone heeft dit bevestigd, dat de gegevens in deze database deels (te weten: voor wat betreft het [VERTROUWELIJK: identifier]) worden versleuteld.<sup>93</sup> Vodafone verklaart dat gegevens ouder dan zeven dagen automatisch en volledig zijn geaggregeerd (op dagbasis) en gedurende ten minste één maand worden bewaard.<sup>94</sup>

Met de term “aggregatie” wordt hier bedoeld aggregatie per protocol, [VERTROUWELIJK], toesteltype [VERTROUWELIJK] of meest bezochte hostnames per dag, week of maand [VERTROUWELIJK].<sup>95</sup> Slechts van de Top[VERTROUWELIJK] *heavy users* is een protocol distributie met dataverbruik beschikbaar (zie **afbeelding 3 en 4** in dit rapport).<sup>96</sup>

AFBEELDING 7: Grafische interface [VERTROUWELIJK]<sup>97</sup>  
[VERTROUWELIJK].

AFBEELDING 8: Grafische interface [VERTROUWELIJK]<sup>98</sup>

Via de grafische interface kunnen onder andere de volgende gegevens worden geraadpleegd: [VERTROUWELIJK] (zie **afbeelding 7 en 8** hierboven).<sup>99</sup>

Ten slotte kan Vodafone rapportages uitdraaien met deze geaggregeerde gegevens.<sup>100</sup>

In haar reactie op een verzoek om aanvullende inlichtingen over de wijze van ‘anonimiseren’ van de gegevens [VERTROUWELIJK] voegt Vodafone daaraan toe: [VERTROUWELIJK].

In de contractdocumentatie van de [VERTROUWELIJK: apparatuur] is een garantiebepaling opgenomen dat de producten en diensten voldoen aan de geldende wettelijke normen die op [VERTROUWELIJK] en Vodafone rusten: [VERTROUWELIJK].

---

apparatuur] 002 tot en met 012. Zie ook Zienswijze 1 Vodafone, p. 21 (doorgenummerde pagina's op de faxbrief): “[VERTROUWELIJK].”

<sup>93</sup> [VERTROUWELIJK] Zie o.a Brief Vodafone van 21 november 2011, p. 3, Bijlage 1 en 2 bij Reactie Vodafone op vordering van 21 februari 2013 (verklaring van de leverancier): “(...) [VERTROUWELIJK].”

<sup>94</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5, Verklaring en print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011. Vgl. ook [VERTROUWELIJK:], p. 17: “[VERTROUWELIJK].”

<sup>95</sup> Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 010 en 005 (**afbeelding 2 en 7** in dit rapport), [VERTROUWELIJK], p. 16 en Zienswijze 1 Vodafone, p. 21 (doorgenummerde pagina's op de faxbrief): “[VERTROUWELIJK] (...)”, (onderstreping door Vodafone).

<sup>96</sup> Zienswijze 1 Vodafone, p. 21 (doorgenummerde pagina's op de faxbrief): “[VERTROUWELIJK].”

<sup>97</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 005.

<sup>98</sup> Idem, [VERTROUWELIJK: apparatuur] 008.

<sup>99</sup> [VERTROUWELIJK], p. 16.

<sup>100</sup> Zie o.a. idem, p. 11 en 18.



[VERTROUWELIJK] Een nieuw, voor Vodafone specifiek project om tot eventuele andere oplossingen te komen is qua tijdsduur en projectkosten minstens van dezelfde omvang als [VERTROUWELIJK]

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de met de [VERTROUWELIJK: apparatuur] voor dit ‘subdoeleinde’ netwerkplanning verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

Vodafone heeft het CBP bij brief van 13 juni 2013, na het sluiten van het onderzoek, medegedeeld dat de [VERTROUWELIJK: apparatuur] sinds vorig jaar niet meer in gebruik is. [VERTROUWELIJK].

### [VERTROUWELIJK]

Vodafone heeft de [VERTROUWELIJK: apparatuur] in 2009 aangeschaft.<sup>101</sup>

De [VERTROUWELIJK: apparatuur] wordt door Vodafone gebruikt voor het monitoren en beheren van het netwerk en de capaciteit daarvan<sup>102</sup>, om op geaggregeerd en geanonimiseerd niveau inzicht te krijgen in het gedrag van groepen klanten zoals de top[VERTROUWELIJK] van meest bezochte websites en meest gebruikte toestellen.<sup>103</sup> Uit de (contracts)documentatie volgt dat de data-analyse apparatuur, zoals gebruikt door Vodafone, in staat is om: [VERTROUWELIJK]

AFBEELDING 9 Grafische interface [VERTROUWELIJK: apparatuur]<sup>104</sup>  
[VERTROUWELIJK]

De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze gegevens verzamelt<sup>105</sup>, vastlegt<sup>106</sup> en bewaart<sup>107</sup> over het bezoek van Vodafone abonnees aan websites en het gebruik van (een aantal) vooraf gedefinieerde apps en protocollen, zoals [VERTROUWELIJK] peer-to-peer, file transfer, [VERTROUWELIJK] web browsing, [VERTROUWELIJK], VoIP [VERTROUWELIJK].<sup>108</sup>

Vodafone verklaart dat *“geen enkele medewerker van Vodafone in staat is om de geaggregeerde data in [VERTROUWELIJK: apparatuur] te herleiden naar of te koppelen aan een geïdentificeerde of identificeerbare natuurlijk persoon. De betreffende data voldoen dus niet aan de beschrijving van het begrip persoonsgegevens in de zin van de Wbp. Vodafone is niet, of in ieder geval niet zonder onevenredige inspanning, in staat om de geaggregeerde data om te zetten in persoonsgegevens. (...) [VERTROUWELIJK].”*<sup>109</sup>

---

<sup>101</sup> Vgl. [VERTROUWELIJK].

<sup>102</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 2.

<sup>103</sup> Idem, p. 1.

<sup>104</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 001.

<sup>105</sup> Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 21 november 2011.

<sup>106</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 001 en E-mail Vodafone van 10 juli 2012.

<sup>107</sup> Idem. Zie ook [VERTROUWELIJK].

<sup>108</sup> [VERTROUWELIJK], p. 9.

<sup>109</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 1-2.

Vodafone verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement (afhankelijk van de websites die zij bezoeken of apps en protocollen die zij gebruiken) enerzijds het [VERTROUWELIJK: identifiërs] en anderzijds [VERTROUWELIJK] de URL en hostname (URL op hoöfddomein) van de website/app<sup>110</sup> of het IP-adres van-naar met poortnummer/protocol<sup>111</sup>, evenals aantallen bytes (volume)<sup>112</sup>, starttijd en eindtijd sessie/tijdsvenster.<sup>113</sup>

Vervolgens worden de gegevens [VERTROUWELIJK] gedurende één uur in niet-persistent geheugen verwerkt. [VERTROUWELIJK].<sup>114</sup>

De bewaartermijnen van de geaggregeerde gegevens waren bij aanvang van het onderzoek:

- uuraggregatie: 15 dagen
- dagaggregatie: 62 dagen
- maandaggregatie: 24 maanden<sup>115</sup>

Via de grafische interface kunnen bijvoorbeeld de volgende gegevens worden geraadpleegd [VERTROUWELIJK].<sup>116</sup>

AFBEELDING 10 Grafische interface [VERTROUWELIJK]<sup>117</sup>  
[VERTROUWELIJK]

AFBEELDING 11 Grafische interface [VERTROUWELIJK]<sup>118</sup>  
[VERTROUWELIJK]

Ten slotte kan Vodafone rapportages uitdraaien met deze geaggregeerde gegevens.<sup>119</sup>

---

<sup>110</sup> De categorieën [VERTROUWELIJK]. Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 21 november 2011.

<sup>111</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5. De categorieën [VERTROUWELIJK]. Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 21 november 2011. Zienswijze 1 Vodafone, p. 24 (doorgenummerde pagina's op de faxbrief): "[VERTROUWELIJK]"

<sup>112</sup> Zie o.a. de categorieën [VERTROUWELIJK]. Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 21 november 2011.

<sup>113</sup> Zie o.a. de categorieën [VERTROUWELIJK]. Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 21 november 2011.

<sup>114</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 10.

<sup>115</sup> Zienswijze 1 Vodafone, p. 25 (doorgenummerde pagina's op de faxbrief). Vgl. [VERTROUWELIJK].

<sup>116</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 001 en [VERTROUWELIJK], p. 8-9. Zie ook Screenshots 2 en 3 Vodafone, bijlage bij Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011 (**afbeelding 10 en 11** hieronder).

<sup>117</sup> Screenshot 2 Vodafone, bijlage bij Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011.

<sup>118</sup> Screenshot 3 Vodafone, idem.

<sup>119</sup> Screenshots Vodafone, bijlage bij Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, Brief Vodafone van 21 november 2011, p. 4 en [VERTROUWELIJK], p. 8.

[VERTROUWELIJK]

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de met de [VERTROUWELIJK: apparatuur] voor dit ‘subdoeleinde’ netwerkplanning verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

### **Getroffen maatregelen**

[VERTROUWELIJK]

Vodafone heeft de bewaartermijnen van de geaggregeerde gegevens verkort tot:

- uuragregatie: 14 dagen
- dagaggregatie: 32 dagen
- maandaggregatie: 13 maanden<sup>120</sup>

[VERTROUWELIJK]

### **Aanleiding toepassing data-analyse technieken netwerkmonitoring**

Vodafone gebruikt de [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] ten behoeve van netwerkmonitoring.<sup>121</sup>

Vodafone verklaart dat het verkrijgen van gegevens met betrekking tot het mobiele dataverkeer door middel van data-analyse technieken noodzakelijk is voor netwerkmonitoring: *“Het gevolg van het niet kunnen toepassen van de technologie zou zijn dat het netwerk (...) instabieler wordt, en dat verstoringen minder goed kunnen worden voorkomen, langer zullen duren en ook pas later worden opgemerkt, waardoor de impact van storingen aanzienlijk groter zal zijn. Gevolg is dus een verslechterde kwaliteit van dienstverlening en hogere kosten - uiteindelijk ook voor de eindgebruiker.”*<sup>122</sup>

Vodafone geeft in haar zienswijze 2 nog een aantal voorbeelden om de noodzakelijkheid van de inzet van de [VERTROUWELIJK: apparatuur] in zijn huidige vorm aan te tonen, juist voor het vroegtijdig signaleren van netwerkproblemen.<sup>123</sup>

Samengevat weergegeven:

[VERTROUWELIJK]

### **Data-analyse apparatuur netwerkmonitoring**

De [VERTROUWELIJK: apparatuur] wordt door Vodafone [VERTROUWELIJK] gebruikt voor het monitoren van het netwerk en om problemen in het netwerk te detecteren en op te lossen<sup>124</sup>. De [VERTROUWELIJK: apparatuur] heeft als instelling dat deze gegevens (‘meldingen’) verzamelt, vastlegt en bewaart<sup>125</sup> om per abonnee en per groep abonnees als er problemen zijn met het afleveren of ontvangen van verkeer

---

<sup>120</sup> Zienswijze 1 Vodafone, p. 25 (doorgenummerde pagina’s op de faxbrief).

<sup>121</sup> Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011 en Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 4-5.

<sup>122</sup> Zienswijze 1 Vodafone, p. 33 (doorgenummerde pagina’s op de faxbrief).

<sup>123</sup> Zienswijze 2 Vodafone, p. 57.

<sup>124</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>125</sup> Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 22 november 2011. Vgl. ook Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5.

in het netwerk de gebruikservaring in kaart te brengen.<sup>126</sup>

Vodafone gebruikt niet alle data-analyse technieken opties/[VERTROUWELIJK: apparatuur] modules.<sup>127</sup>

[VERTROUWELIJK]

Technisch vindt de data-analyse als volgt plaats.

[VERTROUWELIJK]

Vodafone verzamelt (aldus) van al haar abonnees met een (prepaid of postpaid) data abonnement (afhankelijk van problemen met het afleveren of ontvangen van verkeer in het netwerk) enerzijds het [VERTROUWELIJK: identifiers] en anderzijds per [VERTROUWELIJK] een beperkte set aan *counters* (waaronder [VERTROUWELIJK]).<sup>128</sup>

In de [VERTROUWELIJK] apparatuur worden de gegevens (daarna) uitsluitend als op vijftien minuten basis geaggregeerde data opgeslagen.<sup>129</sup>

Via de grafische interface kunnen bijvoorbeeld de volgende gegevens worden geraadpleegd: [VERTROUWELIJK]

AFBEELDING 12 Grafische interface [VERTROUWELIJK]<sup>130</sup>  
[VERTROUWELIJK]

In haar reactie op een verzoek om inlichtingen over de vraag of en zo ja, welke gegevens de [VERTROUWELIJK: apparatuur] vastlegde en bewaarde, schrijft Vodafone: *“Data wordt zeven dagen bewaard en daarna automatisch gewist.”*<sup>131</sup> Vodafone licht nader toe: de op vijftien minuten basis geaggregeerde data per abonnee werden bij aanvang van het onderzoek zeven dagen bewaard. De op dagbasis geaggregeerde data per abonnee werden (vervolgens) 90 dagen bewaard, de op weekbasis geaggregeerde data per abonnee een jaar en de op maandbasis geaggregeerde data twee jaar.<sup>132</sup>

---

<sup>126</sup> [VERTROUWELIJK: apparatuur] Product Description, p. 13 en E-mail Vodafone van 10 juli 2012.

<sup>127</sup> Vodafone overzicht van [VERTROUWELIJK: apparatuur] van 28 oktober 2011.

<sup>128</sup> Zienswijze 1 Vodafone, p. 26 (doorgenummerde pagina's op de faxbrief): *“[VERTROUWELIJK]”* Vodafone overzicht van categorieën van gegevens [VERTROUWELIJK: apparatuur], bijlage bij E-mail Vodafone van 22 november 2011.

<sup>129</sup> E-mail Vodafone van 10 juli 2012.

<sup>130</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 004.

<sup>131</sup> Vodafone verzoek om inlichtingen van 12 september 2012, p. 5.

<sup>132</sup> Vodafone overzicht bewaartermijnen [VERTROUWELIJK: apparatuur], bijlage bij E-mail van 28 oktober 2011. Dit overzicht noemt (nog) een bewaartermijn van vijftien dagen voor vijftien minuten geaggregeerde [VERTROUWELIJK] data. Zie ook idem voor een afwijkende bewaartermijn ten aanzien van *groups*/(groot)zakelijke klanten: de vijftien minuten geaggregeerde data per abonnee werden bij aanvang van het onderzoek dertig dagen bewaard.

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit ‘subdoeleinde’ netwerkmonitoring verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

### **Getroffen maatregelen**

Vodafone heeft naar aanleiding van het onderzoek de bewaartermijnen voor wat betreft de verschillende aggregatieniveaus verkort tot:

Twee dagen (op vijftien minuten basis geaggregeerde data): [VERTROUWELIJK].<sup>133</sup>

Twee weken (op dagbasis geaggregeerde data): [VERTROUWELIJK].<sup>134</sup>

Tien weken (op weekbasis geaggregeerde data): [VERTROUWELIJK].<sup>135</sup>

Zes maanden<sup>136</sup> (op maandbasis geaggregeerde data): [VERTROUWELIJK].

Vodafone licht in haar reactie op de vordering van het CBP toe dat [VERTROUWELIJK]

Aanleiding toepassing data-analyse technieken video-optimalisatie

Vodafone verklaart dat video-optimalisatie wordt gebruikt om de belasting van het netwerk te verminderen en zodat haar klanten minder lang hoeven te wachten voordat zij een video kunnen gaan kijken.<sup>137</sup>

Vodafone verklaart dat video-optimalisatie noodzakelijk is voor het zo efficiënt mogelijk beheren van het netwerk.<sup>138</sup> Vodafone verklaart: *“een groot gedeelte van onze klanten [kijkt, toevoeging door het CBP] bijvoorbeeld video’s niet tot het eind af. Daarom kiezen wij er in sommige gevallen voor om video’s in gedeeltes in te laden. Dit heeft een aantal voordelen voor de gebruiker en voor Vodafone: aan de ene kant wordt het netwerk minder belast, aan de andere kant gebruikt de klant minder data en kan dus langer doen met een bundel. Dit is bij uitstek een voorbeeld hoe Vodafone het inspecteren van protocollen inzet om het netwerk zo efficiënt mogelijk te beheren en aan de juiste protocollen de juiste breedte toe te kennen.”*<sup>139</sup> En: *“Voor een video van vijf minuten is een bepaald volume aan datapakketjes nodig. Door middel van [VERTROUWELIJK: apparatuur] wordt de benodigde hoeveelheid data gereguleerd. In plaats van dat het totale datavolume dat nodig is om de film te bekijken in een keer wordt getransporteerd, wordt steeds een gedeelte van het totale volume aan data getransporteerd. Dit gedeelte is genoeg om het volgende stukje van een film te bekijken. Als iemand na twee minuten stopt met kijken is niet onnodig data getransporteerd voor de resterende drie minuten van de film. Door [VERTROUWELIJK: apparatuur] te gebruiken vermindert Vodafone de belasting van het netwerk en hoeft een klant minder lang te wachten voor hij of zij een video kan gaan kijken.”*<sup>140</sup>

<sup>133</sup> Zie o.a. E-mail van Vodafone van 10 juli 2012 en Zienswijze 2 Vodafone, p. 34.

<sup>134</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 16-17.

<sup>135</sup> Idem, p. 16.

<sup>136</sup> Zienswijze 1 Vodafone, p. 26 (doorgenummerde pagina’s op de faxbrief) en Reactie Vodafone op vordering van 21 februari 2013, p. 15-16.

<sup>137</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 7.

<sup>138</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>139</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>140</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 7.

### Data-analyse apparatuur video-optimalisatie

Vodafone gebruikt de [VERTROUWELIJK] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK] ten behoeve [VERTROUWELIJK] video-optimalisatie en het optimaliseren van webpagina's.<sup>141</sup>

Technisch vindt de data-analyse als volgt plaats.

[VERTROUWELIJK]

Vodafone verklaart daarover: "[VERTROUWELIJK]"<sup>142</sup>

Vodafone verklaart dat de fabrieksinstellingen van de gebruikte [VERTROUWELIJK: apparatuur] niet door of ten behoeve van Vodafone zijn gewijzigd.<sup>143</sup>

De door Vodafone gebruikte [VERTROUWELIJK] apparatuur slaat geen gegevens op en doet geen gegevens opslaan, met uitzondering van logfiles bij foutmeldingen.<sup>144</sup>

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

### Informatie voor abonnees

Het oude Privacy Statement van Vodafone bevatte de volgende informatie over de verwerking van gegevens ten behoeve van verkeersbeheer:

*"Voorbeelden van persoonsgegevens die Vodafone verwerkt zijn uw naam, adres, woonplaats, telefoonnummer en e-mail adres. Vodafone verwerkt ook technische (log)files, zoals IP-adressen, domeinnamen, browser- of telefoontypes en internetdomeinen. (...)*

*Vodafone verwerkt ook uw verkeersgegevens, ook wel bel- en internetgegevens genoemd. Deze gegevens zijn het resultaat van het feit dat u gebruik maakt van het telefoonnummer en/of de "username" welke aan u is verstrekt. (...)*

*Vodafone verwerkt de informatie voortkomend uit verkeersgegevens, om u zo optimaal mogelijk van dienst te kunnen zijn en te kunnen inspelen op uw persoonlijke behoeften. Deze gegevens stellen ons in staat om onze dienstverlening verder te ontwikkelen, te optimaliseren en u op maat gesneden informatie aan te bieden, bijvoorbeeld per post, via SMS, MMS, e-mail, unified messaging of telemarketing.*

---

<sup>141</sup> Zie o.a. Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3-4 en Brief Vodafone van 21 november 2011, p. 2.

<sup>142</sup> Brief Vodafone van 21 november 2011, p. 2. [VERTROUWELIJK] Idem.

<sup>143</sup> Brief Vodafone van 21 november 2011, p. 1 en Verklaring Vodafone [VERTROUWELIJK: apparatuur] van 18 november 2011.

<sup>144</sup> Idem. Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 6. In de verklaring van 18 november 2011 licht Vodafone toe dat de [VERTROUWELIJK: apparatuur] uitsluitend gegevens opslaat wanneer sprake is van een foutmelding (error) in het afspelen van de media. "[VERTROUWELIJK]" Vodafone voegt daaraan toe: "[VERTROUWELIJK]." Brief Vodafone van 21 november 2011, p. 2. Aanvullend verklaart Vodafone bij brief van 21 november 2011 dat [VERTROUWELIJK].

*Zoals hiervoor al aangehaald verwerkt Vodafone ook uw bel- en/of internetgegevens. Vodafone kan bijhouden wanneer, hoe vaak, hoe lang en eventueel met wie/welke telefoonnummers u belt en/of verbinding heeft. (...) Ook ten behoeve van het verkeersbeheer voor het netwerk en voor gegevens-uitwisseling met telecombedrijven in het buitenland worden gegevens verwerkt”, (onderstreping toegevoegd door het CBP).<sup>145</sup>*

Verder bevatten de oude(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. de volgende informatie:

*“(...) Verkeersgegevens: alle Persoonsgegevens voortkomend uit het gebruik van een Aansluiting zoals: locatie, tijdstip en duur van een oproep en het Nummer van de opgeroepen aansluiting. (...) Vodafone verwerkt Persoonsgegevens, waaronder Verkeersgegevens, voor de doeleinden: (...) verkeersbeheer (...)”<sup>146</sup>*

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

### **Getroffen maatregelen**

Het concept gewijzigde Privacy Statement van Vodafone bepaalt, voor zover voor dit onderzoek van belang:

#### *“Verkeersbeheer en netwerkmanagement*

*Wij gebruiken je bel- en internetgegevens en informatie over hoe het netwerk en jouw telefoon in combinatie met hoe het netwerk werkt. Dit doen we voor het verkeersbeheer van ons netwerk. We kunnen op die manier namelijk in kaart brengen welke capaciteit de soorten websites en applicaties die door onze klanten worden gebruikt innemen. Dat doen we omdat we ernaar streven dat onze klanten altijd een goede telefoonverbinding hebben en op volle snelheid kunnen surfen. Zien wij dat er in het netwerk een storing optreedt of het netwerk overbelast dreigt te raken, dan kunnen we hier snel op inspringen.*

*(...) Door het soort datapakketje te herkennen (bijvoorbeeld een e-mail, een webpagina of een video), kunnen we ervoor zorgen dat het op de juiste manier wordt verzonden, afgeleverd en weergegeven bij de ontvanger. Zo kunnen we een video bijvoorbeeld in delen door het netwerk sturen.(...) op die manier voorkomen we vertraging in het netwerk. Dit is noodzakelijk voor een efficiënt gebruik van het netwerk.*

*Om storingen in het netwerk te kunnen signaleren is het voor Vodafone ook noodzakelijk om het verkeer in ons netwerk te bekijken. Zodra wij een storing ontdekken, omdat het jou bijvoorbeeld niet lukt om een website te openen, kunnen wij het probleem direct oplossen, zodat*

---

<sup>145</sup> Privacy Statement Vodafone Libertel B.V. versie september 2011. URL: <https://my.vodafone.nl/Vodafone/wg20/pdf/privacy.pdf> (URL laatst bezocht op 28 mei 2013).

<sup>146</sup> Zie o.a. artikel 1 en artikel 16, tweede lid, van de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versies november 2011 en 1 februari 2010. URL: [http://www.vodafone.nl/Vodafone/wg20/pdf/VF\\_AlgemeneVoorwaardenConsumentenn\\_3.pdf](http://www.vodafone.nl/Vodafone/wg20/pdf/VF_AlgemeneVoorwaardenConsumentenn_3.pdf); [http://www.vodafone.nl/Vodafone/wg20/pdf/alg\\_voorwaarden\\_particulier\\_20100201.pdf](http://www.vodafone.nl/Vodafone/wg20/pdf/alg_voorwaarden_particulier_20100201.pdf) (URL's laatst bezocht op 28 mei 2013).

*er weinig hinder ontstaat.*

*Ook kijken we naar het totale verkeer van onze klanten, dit doen we anoniem, om bepaalde verkeerstrends te ontdekken en om te zorgen dat we op tijd knelpunten in het netwerk herkennen, zodat we eventueel de netwerkcapaciteit kunnen uitbreiden. Zulke knelpunten kunnen bijvoorbeeld ontstaan bij drukbezochte evenementen, zoals voetbalwedstrijden of festivals.”<sup>147</sup>*

In het nieuwe Privacy Statement van Vodafone (versie augustus 2012) wordt over het vastleggen/bijhouden van gegevens over het dataverkeer opgemerkt, voor zover voor dit onderzoek van belang:

*“Wanneer je internet, onderweg of thuis, verwerkt het netwerk ook gegevens over jouw internet verkeer. Gegevens die we onder andere verwerken is het Vodafone e-mailadres dat je bij een Vodafone Thuis abonnement hebt gekregen, de website die je bezoekt, de pagina's waarop je binnen de website doorklikt naar een andere pagina, hoe lang je surft, hoeveel data je downloadt en, wanneer je mobiel internet gebruikt, via welke zendmast je het Vodafone netwerk gebruikt. (...)*

*Wij gebruiken je bel-, en internetgegevens en informatie over hoe het netwerk en jouw telefoon in combinatie met het netwerk werkt. Deze informatie wordt uit het netwerk verkregen door data analyse technieken te gebruiken. Deze analysetechnieken zijn ook wel bekend onder de naam (deep) packet inspection. Dit doen we voor het verkeersbeheer van ons netwerk. We kunnen op die manier namelijk in kaart brengen welke capaciteit de soorten websites en applicaties die door onze klanten worden gebruikt innemen.*

*Internetverkeer bestaat uit datapakketjes. Door het soort datapakketje te herkennen (bijvoorbeeld een e-mail, een webpagina of een video), kunnen we ervoor zorgen dat het op de juiste manier wordt verzonden, afgeleverd en weergegeven bij de ontvanger. Zo kunnen we een video in delen door het netwerk sturen. Voor een e-mail of statusupdate is namelijk een andere bandbreedte nodig dan voor een video of een VoIP-gesprek en op die manier voorkomen we vertraging in het netwerk. Dit is noodzakelijk voor een efficiënt gebruik van het netwerk. Om storingen zo vroeg mogelijk in het netwerk te kunnen signaleren is het voor Vodafone ook noodzakelijk om het verkeer in ons netwerk te bekijken. Dit doen we door ervoor te zorgen dat er automatisch een alarmsignaal wordt afgegeven zodra zich in het netwerk een bepaalde afwijking voordoet. Zodra wij een dergelijk alarmsignaal ontvangen kunnen we nagaan wat er aan de hand is en het (eventuele) probleem voorkomen of direct oplossen, zodat er weinig of zelfs helemaal geen hinder ontstaat. Het monitoren van het verkeer gebeurt op samengesteld of geaggregeerd niveau.*

*Ook kijken we naar het totale verkeer van onze klanten, dit doen we anoniem, om bepaalde verkeerstrends te ontdekken en om te zorgen dat we op tijd knelpunten in het netwerk herkennen, zodat we eventueel de netwerkcapaciteit kunnen uitbreiden. Zulke knelpunten kunnen bijvoorbeeld ontstaan bij drukbezochte evenementen, zoals voetbalwedstrijden of festivals.”<sup>148</sup>*

---

<sup>147</sup> Zienswijze 1 Vodafone, bijlage 5.

<sup>148</sup> Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012. URL: <http://over.vodafone.nl/vodafone-nederland/privacy-veiligheid/privacy-statement> (URL laatst bezocht op 29 mei 2013).



Verder bevatten de nieuwe(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. de volgende informatie:

*“Vodafone verwerkt jouw persoons- en bel- en internetgegevens binnen de kaders van de toepasselijke wet- en regelgeving, in het bijzonder de Telecommunicatiewet en de Wet bescherming persoonsgegevens. Dat doet Vodafone op een wijze en voor de doeleinden zoals beschreven in de meest recente versie van het ‘privacy statement’ (zie [vodafone.nl/privacy](http://vodafone.nl/privacy)). (...)*

#### *Netwerkmanagement*

*Bij het leveren van mobiel internet komt veel kijken. Om te zorgen dat ons netwerk betrouwbaar is, moet het zorgvuldig beheerd worden. Vodafone en andere mobiele aanbieders passen daarom netwerkmanagement technieken toe waarmee de datapakketjes, die door gebruikers worden verstuurd, kunnen worden geanalyseerd. Vodafone kan netwerkmanagement om een aantal redenen toepassen, deze worden hieronder beschreven. (...)*

#### *Voorkomen dat het netwerk volloopt (congestie)*

*Vodafone houdt steeds in de gaten dat overal in het netwerk voldoende capaciteit beschikbaar is. Wij houden bij waar in de toekomst te weinig capaciteit dreigt te ontstaan en breiden dan het aantal antennes uit, of zorgen voor meer frequentieruimte. We doen ons best dat je altijd optimaal gebruik kunt maken van je mobiele internetverbinding.*

*Helaas is het altijd mogelijk dat het toch druk op een bepaalde plek in het netwerk is en congestie optreedt. In dat geval kan verkeer in goede banen geleid worden door toepassing van data-analyse technieken. Een voorbeeld hiervan zijn bepaalde toepassingen, zoals het versturen van een e-mail, met een paar milliseconden vertragen zodat andere toepassingen, zoals een VoIP gesprek, goed blijven functioneren. Op dit moment past Vodafone dit soort technieken nog niet toe, maar zij kan hier in de toekomst wel gebruik van gaan maken.*

#### *Een goede gebruikservaring*

*Door netwerkmanagement kunnen we bepaalde toepassingen herkennen en deze vervolgens op de beste manier door het netwerk sturen. Zo zien we bijvoorbeeld of iemand een smartphone of een tablet gebruikt.*

*Met geavanceerde beeldoptimalisatie- en compressietechnieken zorgen we vervolgens dat de resolutie van afbeeldingen en films, die je bekijkt op internet, precies aansluit bij de resolutie van je beeldscherm. Hierdoor werkt de toepassing optimaal en wordt voorkomen dat het netwerk onnodig volloopt. Bovendien verbruikt je toestel minder data zodat jij uiteindelijk goedkoper uit bent.”<sup>149</sup>*

#### **(Algemene) technische en organisatorische maatregelen**

Vodafone verklaart in reactie op een verzoek om inlichtingen van OPTA een combinatie van technische en organisatorische maatregelen te hanteren,

---

<sup>149</sup> Zie artikel 13 van en de bijlage bij de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versie oktober 2012 en de Algemene Voorwaarden voor Consumenten Vodafone Libertel B.V. Versie maart 2013. URL: <http://www.vodafone.nl/Vodafone/wg20/pdf/algemenevoorwaarden.pdf> en [http://www.vodafone.nl/Vodafone/wg30/pdf/klantenservice/voorwaarden/Algemene\\_voorwaarden\\_Vodafone\\_Red.pdf](http://www.vodafone.nl/Vodafone/wg30/pdf/klantenservice/voorwaarden/Algemene_voorwaarden_Vodafone_Red.pdf) (URL's laatst bezocht op 28 mei 2013).

waaronder uitgebreide autorisatie, authenticatie en logging processen, onder andere gebaseerd op de ISO 27001 beveiligingsstandaard: "[VERTROUWELIJK]".<sup>150</sup>

## 2.5 Facturering

Als onderdeel van het verzamel- en verwerkingsdoeleinde verkeersbeheer en facturering noemt Vodafone facturering. Het gaat hierbij om handhaving van de Dienstvoorwaarden Vodafone BloX, handhaving van de Fair Use Policy, en om MMS- en prepaidverkeer (dat wil zeggen: de facturering van MMS-verkeer en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites).<sup>151</sup> Vodafone gebruikt de [VERTROUWELIJK: apparatuur] voor het doeleinde van facturering, onder te verdelen in: handhaven van dienstvoorwaarden BloX die het gebruik van bepaalde protocollen uitsluiten; handhaving van de fair use policy; voorkomen van billshock; facturering van MMS-verkeer en doorleiden van prepaid abonnees naar (gratis) betaalwebsites.

### Dienstvoorwaarden Vodafone BloX

[VERTROUWELIJK] Vodafone gebruikt de gegevens over het dataverkeer ter handhaving van de Dienstvoorwaarden Vodafone BloX. Dat wil zeggen dat om ongeoorloofd gebruik of misbruik van het datanetwerk te voorkomen/bestrijden (peer-to-peer misbruik en excessieve overschrijdingen van de Fair Use Policy)<sup>152</sup> bij prepaid of postpaid data-abonnementen waarop Dienstvoorwaarden Vodafone BloX van toepassing zijn<sup>153</sup> als de abonnee gebruik maakt van een protocol waartoe hij niet is gerechtigd de snelheid van de verbinding (uiteindelijk) wordt verlaagd.<sup>154</sup> Vodafone licht toe: "[VERTROUWELIJK]"<sup>155</sup> Vodafone verklaart dat deze verwerking is gebaseerd op toestemming.<sup>156</sup>

Vodafone verklaart met betrekking tot de handhaving van de Dienstvoorwaarden Vodafone BloX verder: "[VERTROUWELIJK]", (onderstreping toegevoegd door het CBP).<sup>157</sup>

Vanwege de beëindiging/uitfasering van deze Dienstvoorwaarden Vodafone BloX is/wordt de gegevensverwerking voor dat doeleinde in dit onderzoek niet door het CBP beoordeeld.

---

<sup>150</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 3.

<sup>151</sup> Idem, p. 1-2 en Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 1, 3 en 8-10. Vodafone verklaart daarin ook: "*Vodafone maakt wel degelijk gebruik van packet inspection om MSS verkeer te factureren. Zoals Vodafone hiervoor heeft uitgelegd schaaft zij dit gebruik onder het doeleinde 'verkeersbeheer en facturering'.*" Idem, p. 8. Vgl. ook Brief Vodafone van 21 november 2011, p. 5.

<sup>152</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>153</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>154</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 6.

<sup>155</sup> Idem.

<sup>156</sup> "[VERTROUWELIJK]". Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 1.

<sup>157</sup> Verklaring Vodafone met betrekking tot de handhaving van de Dienstvoorwaarden Vodafone BloX van 21 november 2011. Bijlage bij e-mail van Vodafone van 21 november 2011.

### **Billshock en (ter naleving van) de Europese roaming regulering**

Vodafone gebruikt de [VERTROUWELIJK]-apparatuur om klanten te kunnen behoeden voor de zogeheten 'billshock' en hen, via monitoring van het dataverkeer, tijdig te kunnen waarschuwen dat zij hun data roaming cap van 50 euro bijna hebben bereikt (ter naleving van de Europese roaming regulering).<sup>158</sup>

De inzet van data-analyse technieken om abonnees te behoeden voor de zogenaamde 'billshock' en hen tijdig te (kunnen) waarschuwen dat zij hun data roaming cap van 50 euro bijna hebben bereikt (anders gezegd: de gegevensverwerking in verband met data roaming verkeer), valt buiten de scope van dit onderzoek.

### **MMS-verkeer**

MMS (*Multimedia Messaging Service*) is de multimediale opvolger van SMS. De [VERTROUWELIJK: apparatuur] verzamelt gegevens over het mobiele dataverkeer van alle Vodafone abonnees om daaruit MMS-verkeer te herkennen.<sup>159</sup>

[VERTROUWELIJK] Voor MMS-verkeer geldt een vast tarief per bericht. Om dubbele facturering van MMS-verkeer te voorkomen, wordt binnen de volumemeting van dataverkeer het MMS-gerelateerde volume als gratis aangemerkt. Om dit MMS-verkeer te herkennen worden data-analyse technieken toegepast.<sup>160</sup>  
[VERTROUWELIJK]

Er vindt voor dit doeleinde geen (aanvullende) opslag plaats van gegevens over of uit het dataverkeer.<sup>161</sup>

De inzet van data-analyse technieken valt buiten de scope van dit onderzoek voor zover het de facturering van MMS-verkeer betreft.<sup>162</sup>

### **Prepaidverkeer**

Vodafone gebruikt de [VERTROUWELIJK: apparatuur]-apparatuur tevens om verkeer van prepaidklanten naar (gratis) opwaardeersites te transporteren bij een ontoereikend prepaid tegoed.<sup>163</sup>

Een prepaidklant betaalt realtime voor het gebruik van diensten. Vodafone houdt het tegoed van prepaidklanten bij in een factureringssysteem [VERTROUWELIJK]. Als een prepaidklant een datasessie wil starten, herkent de [VERTROUWELIJK] deze abonnee als prepaidklant. Voordat een verbinding wordt opgebouwd, vraagt de [VERTROUWELIJK] aan het factureringssysteem ('prepaid systeem') of de prepaidklant nog voldoende tegoed heeft. Als het tegoed van de abonnee

---

<sup>158</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3.

<sup>159</sup> Idem, p. 8. Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011. Zie ook bijlage 2 bij Reactie Vodafone op verzoek om inlichtingen van 12 september 2011.

<sup>160</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 8 en bijlage 2 bij deze reactie.

<sup>161</sup> Idem.

<sup>162</sup> Het is niet onwaarschijnlijk dat de MMS-dienst, gelet op het gebruik dat daarvan in het algemeen wordt gemaakt, van steeds minder groot belang wordt/is.

<sup>163</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 8-9 en bijlage 3 bij deze reactie. Verklaring Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011.

ontoereikend is, geeft het prepaid systeem geen toestemming voor een verbinding en zal de datasessie niet slagen. Er is dan alleen toegang mogelijk tot gratis opwaardeersites totdat het tegoed is opgewaardeerd.<sup>164</sup>

Bij een 'gratis' URL vraagt de [VERTROUWELIJK] niet aan het factureringssysteem of de abonnee nog voldoende tegoed heeft. Om gratis URL's te herkennen worden data-analyse technieken toegepast<sup>165</sup>: "[VERTROUWELIJK]"<sup>166</sup>

Er vindt voor dit doeleinde geen opslag plaats van gegevens over of uit het dataverkeer.<sup>167</sup>

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit 'subdoeleinde' het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

### **Informatie voor abonnees**

Het oude Privacy Statement van Vodafone bevatte de volgende informatie over de verwerking van gegevens ten behoeve van de facturering van MMS- en prepaidverkeer:

*"Zoals hiervoor al aangehaald verwerkt Vodafone ook uw bel- en/of internetgegevens. Vodafone kan bijhouden wanneer, hoe vaak, hoe lang en eventueel met wie/welke telefoonnummers u belt en/of verbinding heeft. Vodafone verwerkt deze gegevens om aan u een (gespecificeerde) factuur te kunnen sturen (...)."*<sup>168</sup>

Verder bevatten de oude(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. de volgende informatie:

*"Vodafone verwerkt Persoonsgegevens, waaronder Verkeersgegevens, voor de doeleinden: facturatie, debiteuren-administratie, betalingen voor interconnectie en bijzondere toegang (...)."*<sup>169</sup>

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

---

<sup>164</sup> Bijlage 3 bij Reactie Vodafone op verzoek om inlichtingen van 12 september 2011.

<sup>165</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 8.

<sup>166</sup> Idem, p. 9.

<sup>167</sup> Vgl. bijlage 3 bij Reactie Vodafone op verzoek om inlichtingen van 12 september 2011.

<sup>168</sup> Privacy Statement Vodafone Libertel B.V. versie september 2011.

<sup>169</sup> Zie artikel 16, tweede lid, van de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versies november 2011 en 1 februari 2010. URL: [http://www.vodafone.nl/Vodafone/wg20/pdf/VF\\_AlgemeneVoorwaardenConsumentenn\\_3.pdf](http://www.vodafone.nl/Vodafone/wg20/pdf/VF_AlgemeneVoorwaardenConsumentenn_3.pdf); [http://www.vodafone.nl/Vodafone/wg20/pdf/alg\\_voorwaarden\\_particulier\\_20100201.pdf](http://www.vodafone.nl/Vodafone/wg20/pdf/alg_voorwaarden_particulier_20100201.pdf) (URL's laatst bezocht op 28 mei 2013).

## Getroffen maatregelen

Vodafone verleent thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK].<sup>170</sup>

Het concept gewijzigde Privacy Statement van Vodafone bepaalt, voor zover voor dit onderzoek van belang:

### *"Facturering en voorwaarden*

*(...) Voor het in rekening brengen van de kosten van een MMS bericht is het voor ons facturatie systeem noodzakelijk om te kunnen zien dat je een MMS hebt verstuurd. Want bij een MMS wordt er data door het netwerk verstuurd die wij niet bij je in rekening willen brengen. We brengen alleen het bedrag voor de MMS bij je in rekening.*

*Als je prepaid tegoed op is en je wilt dit via een mobiele internet pagina opladen kijkt ons systeem naar het data verkeer. We brengen het verkeer naar deze websites namelijk niet bij je in rekening, dan zou je immers niet naar de website kunnen surfen omdat je tegoed op is."*<sup>171</sup>

In het nieuwe Privacy Statement van Vodafone (versie augustus 2012) wordt over de facturering van MMS- en prepaidverkeer opgemerkt, voor zover voor dit onderzoek van belang:

### *"3.4.1 Het factureren van MMS berichten*

*Bij Vodafone betaal je een vast bedrag voor een MMS bericht. In dat bedrag zijn de verzendkosten van deze berichten niet meegenomen. Bij het versturen van MMS berichten wordt er data door het netwerk verstuurd en daar zijn ook kosten aan verbonden, maar die kosten willen we niet bij je in rekening brengen. Om er ervoor te zorgen dat je alleen de kosten voor het MMS bericht zelf betaalt en niet de verzendkosten daarvan, is het noodzakelijk dat ons facturatiesysteem in het netwerk herkent dat het om een MMS bericht gaat. Alleen dan zijn we in staat om alleen het MMS bericht zelf in rekening te brengen en niet ook de verzendkosten daarvan.*

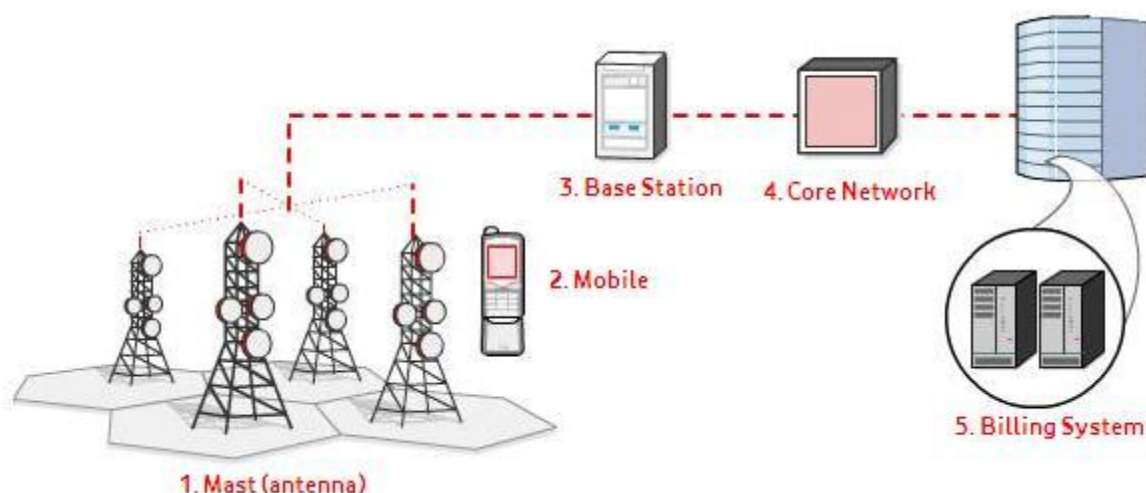
### *3.4.2 Het opwaarderen van prepaid tegoed*

*Als je prepaid tegoed op is en je wilt dit via een mobiele internet pagina opladen, kijkt ons systeem naar het data verkeer. We brengen het verkeer naar deze websites namelijk niet bij je in rekening, dan zou je immers niet naar de website kunnen surfen omdat je tegoed op is. Onderstaand een overzicht hoe ons betaalproces in het netwerk verloopt.*

---

<sup>170</sup> Zienswijze 2 Vodafone, p. 10.

<sup>171</sup> Zienswijze 1 Vodafone, bijlage 5.



1. *Zendmast (antenne). In de mast worden verschillende gegevens verwerkt. Deze masten staan verspreid door heel Nederland en hebben allemaal hun eigen exacte geografische locatie. Vodafone moet jouw mobiele nummer linken aan de antenne om je gesprek op te kunnen zetten of een bericht af te leveren. Je telefoon is aangemeld op een mast en daaruit kunnen we de locatie van je telefoon in het netwerk afleiden. Naast dat we deze gegevens nodig hebben om bijvoorbeeld gesprekken op te zetten, kan deze informatie ook worden gebruikt om hulpdiensten in staat te stellen je te vinden, natuurlijk alleen als dat noodzakelijk is.*
2. *De telefoon. Telkens als je je telefoon gebruikt (of Vodafone Mobiel Internet) om een gesprek te voeren, een sms te versturen of het internet op te gaan, wordt informatie over het toestel vastgelegd en door het netwerk gebruikt om dit mogelijk te maken. Ook kijken we welke soort toestellen op ons netwerk worden gebruikt omdat het ene toestel meer capaciteit verbruikt dan het andere. Deze informatie hebben we dus nodig om maatregelen te nemen die congestie kunnen voorkomen. De informatie is alleen beschikbaar op geanonimiseerd en geaggregeerd niveau.*
3. *Base station. In het base station wordt informatie over het gebruik van het netwerk opgeslagen. Deze informatie hebben we nodig om de communicatiestromen van klanten in goede banen te leiden, maar ook om eventueel vragen van jou over technische problemen te kunnen beantwoorden.*
4. *Core network. In het core network wordt informatie bijgehouden om de integriteit en de kwaliteit van het netwerk te waarborgen. Als we bijvoorbeeld zien dat op een bepaalde plek een gesprek vaak afgebroken wordt doordat het netwerk plotseling wegvault, geeft dit aan dat we daar waarschijnlijk een extra mast moeten plaatsen.*
5. *Billing system. In het billing of factureringssysteem worden de gegevens bijgehouden om de rekeningen voor de klanten op te stellen. Bijvoorbeeld hoelang een gesprek heeft geduurd en of er bepaalde diensten van derden zijn gebruikt. (...)."<sup>172</sup>*

<sup>172</sup> Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012.

## 2.6 Beveiliging

Als tweede verzamel- en verwerkingsdoeleinde van gegevens noemt Vodafone beveiliging (voor het gebruik van spam- en virusfilters en het detecteren van botnets in het netwerk, maar ook tegen andere vormen van malware zoals trojans en inbraak pogingen, evenals om de integriteit en veiligheid van haar netwerk(en) en diensten te waarborgen).<sup>173</sup>

### Aanleiding toepassing data-analyse technieken

Vodafone verklaart: *"Door middel van het [VERTROUWELIJK: apparatuur] van [VERTROUWELIJK] beveiligt Vodafone haar netwerk tegen onder meer virussen, trojans en inbraakpogingen. [VERTROUWELIJK]."*<sup>174</sup>

Vodafone verklaart verder ten aanzien van het gebruik van spamfilters: *"[VERTROUWELIJK]."*<sup>175</sup>

### Data-analyse apparatuur

Vodafone gebruikt de [VERTROUWELIJK: apparatuur] van de leverancier [VERTROUWELIJK] voor de beveiliging van het netwerk.<sup>176</sup>

Vodafone inspecteert en analyseert het dataverkeer<sup>177</sup> van al haar abonnees met een (prepaid of postpaid) data abonnement en zorgt ervoor dat spam en virussen/malware tegen worden gehouden en verwijderd.

Er vindt voor dit doeleinde opslag plaats van gegevens over en uit het dataverkeer. Vodafone verklaart dat de logfiles van opgespoorde anomalieën of beveiligingslekken maximaal twee maanden worden bewaard. Daarna worden de logfiles automatisch door het systeem gewist.<sup>178</sup>

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

---

<sup>173</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1. Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 3. Brief Vodafone van 21 november 2011, p. 5.

<sup>174</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5.

<sup>175</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>176</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 4.

<sup>177</sup> Daaronder begrepen inhoud van door abonnees gedownloadte bestanden en verzonden en ontvangen e-mails aan de hand vooraf gedefinieerde spam-, virus- en malwareherkenningsspatronen, voor zover nodig om spam/virussen/malware tegen te houden en te verwijderen (oftewel, spam-, virus- en malwareherkenninggegevens uit de inhoud van het dataverkeer).

<sup>178</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 5.

kijken naar kwaadaardige code.<sup>179</sup>

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde beveiliging verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

### **Informatie voor abonnees**

De oude(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. bevatten de volgende informatie over de verwerking van gegevens ten behoeve van beveiliging:

*"Vodafone verwerkt Persoonsgegevens, waaronder Verkeersgegevens, voor de doeleinden: (...) voorkoming, opsporing en bestrijding van fraude en onregelmatigheden (...)." <sup>180</sup>*

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

### **Getroffen maatregelen**

Ook het concept gewijzigde Privacy Statement bevat geen informatie over spam- en virusfiltering en malwarebestrijding.

In het nieuwe Privacy Statement van Vodafone (versie augustus 2012) wordt over beveiliging opgemerkt, voor zover voor dit onderzoek van belang:

*"Om jouw privacy en de vertrouwelijkheid van jouw gegevens te beschermen, treft Vodafone passende technische en organisatorische maatregelen. Het Vodafone netwerk in Nederland wordt via het Global Security Operations Centrum in Düsseldorf 24/7 in de gaten gehouden. Dit Centrum kan in een vroeg stadium bedreigingen of aanvallen signaleren en actie ondernemen. Daarnaast wordt het hele netwerk structureel gescand op virussen, schadelijke software en inbraakpogingen. Het beheren en beveiligen van waardevolle gegevens is bij Vodafone gebaseerd op de internationaal erkende beveiligingsnorm ISO 27001. Geregeld laat Vodafone deze beveiligingsprocessen door onafhankelijke auditors controleren. (...)" <sup>181</sup>*

Verder bevatten de nieuwe(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. de volgende informatie:

*"Bescherming van jou en het netwerk*

*Vodafone gebruikt netwerkmanagement om computervirussen, malware (bestandjes die schade kunnen toebrengen) en spam (ongevraagde e-mails) tegen te gaan. Als Vodafone hier niets tegen doet, kun je slachtoffer worden van virus- en malware- aanvallen. Deze aanvallen vormen een bedreiging voor je internetveiligheid en gebruikservaring.*

---

<sup>179</sup> Een toelichting op virusbestrijdingstechnieken is te lezen op URL: [http://en.wikipedia.org/wiki/Antivirus\\_software](http://en.wikipedia.org/wiki/Antivirus_software) (URL laatst bezocht op 28 mei 2013).

<sup>180</sup> Zie artikel 16, tweede lid, van de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versies november 2011 en 1 februari 2010.

<sup>181</sup> Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012.



*Bijvoorbeeld omdat je mailbox helemaal volloopt, maar ook omdat het netwerk dan een heel stuk trager wordt door al het onnodige verkeer.”<sup>182</sup>*

## 2.7 Behandeling van verzoeken om inlichtingen van klanten

Als derde verzamel- en verwerkingsdoeleinde van gegevens noemt Vodafone de behandeling van verzoeken om inlichtingen van klanten, om klachten en problemen van klanten op te lossen.<sup>183</sup> Vodafone verklaart: *“voor het behandelen van klantverzoeken maakt Vodafone naast [VERTROUWELIJK: apparatuur] ook gebruik van [VERTROUWELIJK: apparatuur] van [VERTROUWELIJK]”*.<sup>184</sup>

Vodafone gebruikt [VERTROUWELIJK] verschillende soorten data-analyse apparatuur in het kader van de behandeling van verzoeken om inlichtingen van klanten, ter ondersteuning van de klantenservice (te weten: de [VERTROUWELIJK: apparatuur] van de [VERTROUWELIJK] leverancier [VERTROUWELIJK]).<sup>185</sup>

Vodafone slaat voor dit doeleinde enerzijds gegevens op over het dataverkeer van alle abonnees<sup>186</sup> en anderzijds (bij video-optimalisatie) alleen in specifieke, individuele gevallen, bij storingen en fouten.<sup>187</sup>

Vodafone verklaart dat de inzet van de [VERTROUWELIJK: apparatuur] noodzakelijk is om vragen van abonnees met betrekking tot facturen te beantwoorden.<sup>188</sup> *“bijvoorbeeld: ‘ik heb op datum X geen data verbruikt maar heb daarvoor wel een rekening ontvangen.”<sup>189</sup>*

Via de gebruikersinterface kan de afdeling Klantenservice, in geval van de [VERTROUWELIJK: apparatuur], bijvoorbeeld de volgende historische gegevens over het dataverkeer raadplegen: performance informatie en dataverbruik in combinatie met het [VERTROUWELIJK: identifiërs] (zie over de [VERTROUWELIJK: apparatuur] ook paragraaf 2.4 ‘Verkeersbeheer’, onder het kopje ‘[VERTROUWELIJK]’, p. 30 van dit rapport).<sup>190</sup>

Via de gebruikersinterface kunnen de per vijftien minuten geaggregeerde gegevens per abonnee tot vijf dagen terug worden ingezien.<sup>191</sup>

---

<sup>182</sup> Zie de bijlage bij de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versie oktober 2012 en de Algemene Voorwaarden voor Consumenten Vodafone Libertel B.V. Versie maart 2013.

<sup>183</sup> Zie Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 1-2. Brief Vodafone van 21 november 2011, p. 5.

<sup>184</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 4.

<sup>185</sup> Idem, p. 4-5. Zie ook E-mail Vodafone van 5 december 2011.

<sup>186</sup> Dit betreft de [VERTROUWELIJK: apparatuur].

<sup>187</sup> In geval van de [VERTROUWELIJK: apparatuur]: wanneer sprake is van een foutmelding (error) in het afspelen van de media worden “[VERTROUWELIJK].” Brief Vodafone van 21 november 2011, p. 2.

<sup>188</sup> Zienswijze 1 Vodafone, p. 29 (doorgenummerde pagina’s op de faxbrief).

<sup>189</sup> Idem, p. 26 (doorgenummerde pagina’s op de faxbrief).

<sup>190</sup> Print-outs Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011.

<sup>191</sup> Verklaring Vodafone en vastgesteld tijdens het onderzoek ter plaatse van 26 oktober 2011.

Vodafone verklaart dat deze verwerking is gebaseerd op toestemming: "(...), zoals bij het oplossen van klantklachten en handhaven van de in onze eerdere reactie aan Opta reeds genoemde productvoorwaarden. Dit gebeurt echter niet zonder toestemming van klanten, zij worden hier vooraf over geïnformeerd", (onderstreping toegevoegd door het CBP).<sup>192</sup>

Vodafone verklaart dat de [VERTROUWELIJK: apparatuur] niet standaard rapporten aanmaakt over het dataverbruik per abonnee. "Er wordt alleen een rapport gemaakt naar aanleiding van een concrete klantklacht nadat de betrokken abonnee of eindgebruiker Vodafone toestemming heeft gegeven voor het verwerken van deze [VERTROUWELIJK: apparatuur] data."<sup>193</sup>

In **bijlage II** bij dit rapport is een samenvattend overzicht opgenomen in tabelvorm van de voor dit doeleinde behandeling van verzoeken om inlichtingen van klanten verwerkte categorieën van gegevens. Deze bijlage vormt een integraal onderdeel van dit rapport.

### **Informatie voor abonnees**

Het oude Privacy Statement van Vodafone bevatte de volgende informatie over de verwerking van gegevens ten behoeve van de behandeling van verzoeken om inlichtingen van klanten:

*"Vodafone verwerkt voor een beperkte periode de bel-, locatie- en/of internetgegevens om uw vragen over de aan u verstuurde factuur te kunnen beantwoorden in geval van bijvoorbeeld een geschil."*<sup>194</sup>

De oude(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. bevatten de volgende informatie over de verwerking van gegevens ten behoeve van de afhandeling van klantverzoeken:

*"Vodafone verwerkt Persoonsgegevens, waaronder Verkeersgegevens, voor de doeleinden: (...) klachtenafhandeling en geschillenbeslechting, (...), informatie aan Contractant over de eigen Verkeersgegevens (...)." <sup>195</sup>*

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

### **Getroffen maatregelen**

Het concept gewijzigde Privacy Statement van Vodafone bepaalt, voor zover voor dit onderzoek van belang:

*"Voor klachtafhandeling over storingen en vragen over je factuur kan het zo zijn dat we je netwerk gegevens gebruiken. Als je met Vodafone belt over een storing of met een vraag over je factuur en we gebruiken die gegevens dan bespreekt de Vodafone medewerker dat met jou en*

---

<sup>192</sup> Reactie Vodafone op verzoek om inlichtingen van 12 september 2011, p. 1.

<sup>193</sup> E-mail van Vodafone van 10 juli 2012. Vgl. ook Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2: "Deze tools worden alleen met uitdrukkelijke voorafgaande toestemming van een Vodafone eindgebruiker gebruikt om specifieke problemen van een specifieke klant op te lossen."

<sup>194</sup> Privacy Statement Vodafone Libertel B.V. versie september 2011.

<sup>195</sup> Zie artikel 16, tweede lid, van de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versies november 2011 en 1 februari 2010.

*leggen we uit hoe we dit doen. Omdat we hier duidelijk en transparant over willen zijn, kiezen we ervoor jou om toestemming te vragen om in deze gegevens te kunnen kijken. Wij kunnen dan zien of bijvoorbeeld bepaald dataverbruik ook echt is geregistreerd in het netwerk of dat er misschien een storing is opgetreden.”<sup>196</sup>*

In het nieuwe Privacy Statement van Vodafone (versie augustus 2012) wordt over de behandeling van verzoeken om inlichtingen van klanten opgemerkt, voor zover voor dit onderzoek van belang:

#### *“3.4 Rekening betalen - facturering en voorwaarden*

*(...) We bewaren de bel,- en internetgegevens ook voor het geval je vragen of een klacht hebt over je rekening. (...)*

*Voor klachtafhandeling over storingen en vragen over je factuur kan het zo zijn dat we je netwerk gegevens gebruiken. Als je met Vodafone belt over een storing of met een vraag over je factuur en we gebruiken die gegevens dan bespreekt de Vodafone medewerker dat met jou en leggen we uit hoe we dit doen. Omdat we hier duidelijk en transparant over willen zijn, kiezen we ervoor jou om toestemming te vragen om in deze gegevens te kunnen kijken. Wij kunnen dan zien of bijvoorbeeld bepaald dataverbruik ook echt is geregistreerd in het netwerk of dat er misschien een storing is opgetreden. (...)*

#### *3.5 Klantenservice*

*(...) Als je een klacht hebt over het Vodafone netwerk kunnen we je soms beter helpen door gericht te zoeken naar de problemen in het netwerk op de momenten dat jij probeerde te bellen. Hiervoor gebruiken we zogenoemde ruwe netwerk gegevens. Voordat we dit doen zullen we hiervoor je toestemming vragen. (...)”<sup>197</sup>*

## **2.8 Verdere verwerking**

Vodafone gebruikt de rapportages uit de [VERTROUWELIJK: apparatuur] voor het vaststellen van de business strategie van Vodafone.<sup>198</sup> Deze rapportages bevatten de volgende gegevens: [VERTROUWELIJK].<sup>199</sup>

### **Informatie voor abonnees**

Het oude Privacy Statement van Vodafone bevatte de volgende informatie over de verwerking van gegevens ten behoeve van marktonderzoek:

*“Vodafone verwerkt de informatie voortkomend uit verkeersgegevens, om u zo optimaal mogelijk van dienst te kunnen zijn en te kunnen inspelen op uw persoonlijke behoeften. Deze gegevens stellen ons in staat om onze dienstverlening verder te ontwikkelen, (...)*

*4. Bel- en internetgegevens kunnen ook voor marktonderzoek en verkoopactiviteiten van Vodafone worden gebruikt*

<sup>196</sup> Zienswijze 1 Vodafone, bijlage 5.

<sup>197</sup> Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012.

<sup>198</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 1.

<sup>199</sup> Print-out Vodafone tijdens het onderzoek ter plaatse van 26 oktober 2011, [VERTROUWELIJK: apparatuur] 001 en [VERTROUWELIJK], p. 8-9. Zie ook Screenshots 2 en 3 Vodafone, bijlage bij Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011 (**afbeelding 10 en 11** in dit rapport).

*Vodafone streeft er voortdurend naar om haar (mobiele) dienstverlening aan te passen aan de behoefte van haar klanten en waar nodig te verbeteren. Hiervoor doet Vodafone veel onderzoek en luisteren wij naar de wensen van onze klanten. Uw bel- en/of internetgegevens helpen Vodafone bij het ontwikkelen van nieuwe diensten en producten.*

*(...) Mocht u er bezwaar tegen hebben dat Vodafone uw bel- en/of internetgegevens voor marktonderzoek en verkoopactiviteiten gebruikt, dan kunt u dit kenbaar maken door een ongefrankeerde brief te sturen naar:*

*Vodafone Klantenservice o.v.v. "Privacy / bezwaar gebruik verkeersgegevens"  
Antwoordnummer 1500, 6201 BM Maastricht.*

*U kunt ook bellen naar onze Klantenservice 1200.*<sup>200</sup>

De oude(re) Algemene Voorwaarden Consumenten Vodafone Libertel B.V. bevatten de volgende informatie over de verdere verwerking van gegevens ten behoeve van het vaststellen van de business strategie van Vodafone:

*"Met uitzondering van Verkeersgegevens worden Persoonsgegevens ook verwerkt voor marktonderzoek en verkoopactiviteiten met betrekking tot Diensten en andere diensten van Vodafone en/of diensten van derden die te maken hebben met de Diensten."*<sup>201</sup>

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

### **Getroffen maatregelen**

Het concept gewijzigde Privacy Statement bevat geen informatie over de gegevensverwerking voor het vaststellen van de business strategie van Vodafone.

In het nieuwe Privacy Statement van Vodafone (versie augustus 2012) wordt over marketing opgemerkt, voor zover voor dit onderzoek van belang:

*"Wij streven er voortdurend naar om onze(mobiele) dienstverlening aan te passen aan de behoefte van jou als klant van Vodafone en waar nodig te verbeteren. Hiervoor doet Vodafone veel onderzoeken en luisteren wij naar jouw wensen. Jouw bel- en/of internetgegevens helpen Vodafone bij het ontwikkelen van nieuwe diensten en producten, veelal gebruiken we deze op geanonimiseerde wijze. (...) Mocht je liever niet willen dat wij je gegevens voor deze marketingdoeleinden gebruiken, dan kun je ons dit op ieder moment laten weten. Kijk hiervoor onder het kopje "Contact"."*<sup>202</sup>

---

<sup>200</sup> Privacy Statement Vodafone Libertel B.V. versie september 2011.

<sup>201</sup> Zie artikel 16, tweede lid, van de Algemene Voorwaarden Consumenten Vodafone Libertel B.V. Versies november 2011 en 1 februari 2010.

<sup>202</sup> Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012.

### 3. UITWERKING VAN HET WETTELIJK KADER EN BEOORDELING

#### 3.1 Wettelijk kader: samenloop Wbp en Tw

Op de verwerking van persoonsgegevens in de sector elektronische communicatie (telecommunicatiesector) is de algemene privacyrichtlijn 95/46/EG (hierna: Privacyrichtlijn) van toepassing (geïmplementeerd in de Wbp).<sup>203</sup> De Privacyrichtlijn regelt de verwerking van persoonsgegevens en de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, waaronder het recht op (bescherming van de) persoonlijke levenssfeer. Daarnaast gelden de bepalingen uit de richtlijn betreffende privacy en elektronische communicatie 2002/58/EG (hierna: e-Privacyrichtlijn) (geïmplementeerd in de Tw).<sup>204</sup> De e-Privacyrichtlijn regelt de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor gebruikers van openbare elektronische communicatiediensten.<sup>205</sup> 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).<sup>206</sup> Er is geen sprake van een *lex specialis*-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene.<sup>207</sup> 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).<sup>208</sup>

In de wetsgeschiedenis is daarover het volgende opgemerkt:

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

<sup>203</sup> “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.

<sup>204</sup> Zie artikel 1, tweede lid, van de e-Privacyrichtlijn; zie ook overweging 12 van de e-Privacyrichtlijn.

<sup>205</sup> Zie artikel 1, eerste lid, van de e-Privacyrichtlijn; zie ook overwegingen 4, 8 en 12 van de e-Privacyrichtlijn.

<sup>206</sup> 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.”

<sup>207</sup> 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).

<sup>208</sup> Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 45.

van dit artikel 2, geldt de regel «bijzondere wet gaat voor algemene wet» echter niet. De Wbp geldt in deze gevallen immers naast de specifieke wetgeving. Alsdan heeft de Wbp dus een aanvullende werking, namelijk voor die onderdelen die niet door de bijzondere wetgeving worden gedekt. De Organisatiewet sociale verzekeringen 1997 en de Telecommunicatiewet zijn daar een voorbeeld van. De geheimhoudingsvoorschriften in de Organisatiewet sociale verzekeringen vormen dus een uitwerking van die in de Wbp. Wel is het zo dat de voorschriften van de Wbp daarmee niet als direct bindende normen in beeld komen, ze spelen enkel zijdelings een rol.”<sup>209</sup>

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*.<sup>210</sup>

<sup>209</sup> 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).

<sup>210</sup> Overweging 47 van de Privacyrichtlijn luidt in dit verband: “Overwegende dat, wanneer een bericht dat persoonsgegevens bevat, wordt verzonden via een telecommunicatie- of elektronische postdienst waarvan het enige doel is dit soort berichten door te geven, het de persoon is van wie het bericht uitgaat, en niet degene die de dienst aanbiedt, die normaliter zal worden beschouwd als verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk

Vodafone, gevestigd te Maastricht, Nederland, bepaalt de doeleinden van en de middelen voor de verwerking van persoonsgegevens bij de inzet van data-analyse technieken op het dataverkeer over haar mobiele netwerk.<sup>211</sup> Vodafone heeft zich, voor zover voor dit onderzoek van belang, op 13 maart 2008 als verantwoordelijke gemeld bij het CBP.<sup>212</sup> Uit de gegevens uit het Handelsregister volgt dat Vodafone bevoegd is om doel en middelen vast te stellen. Vodafone 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.<sup>213</sup>

#### 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 persoon te identificeren; dat de*

---

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

<sup>211</sup> Zie ook Privacy Statement Vodafone Libertel B.V. Versie: augustus 2012: "De verantwoordelijke voor het verzamelen en gebruiken van je gegevens is Vodafone Libertel B.V., Avenue Céramique in Maastricht."

<sup>212</sup> Zie de melding met nummer m1040032 (versienummer 2.0).

<sup>213</sup> 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".

*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.<sup>214</sup>

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking<sup>215</sup> hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of - gezien de context<sup>216</sup> waarin ze worden verwerkt - medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.<sup>217</sup> 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.<sup>218</sup> 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.<sup>219</sup> Als voorbeeld wordt in de wetsgeschiedenis bij de Wbp genoemd het telefoonnummer.<sup>220</sup>

<sup>214</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.

<sup>215</sup> Zie WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 10-11 en 27. URL:

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_nl.pdf](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

<sup>216</sup> Vgl. idem: Er is sprake van informatie 'betreffende' een persoon "wanneer, rekening houdende met alle omstandigheden van het precieze geval, gegevens worden gebruikt of waarschijnlijk zullen worden gebruikt met het doel een persoon te beoordelen, op een bepaalde wijze te behandelen of de status of het gedrag van die persoon te beïnvloeden", met andere woorden, het doel.

<sup>217</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 46. Vgl. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 11: Er is sprake van informatie 'betreffende' een persoon "indien het gebruik ervan, rekening houdende met alle omstandigheden van het geval, naar verwachting gevolgen zal hebben voor iemands rechten of belangen", met andere woorden, het resultaat.

<sup>218</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 47. "Anders dan de Registratiekamer in haar advies stelt is niet vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt. Indien het daarentegen mogelijk is de gegevens te gebruiken bij voorbeeld om fraude op te sporen, dan is er sprake van persoonsgegevens. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken, ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt."

<sup>219</sup> Idem, p. 46-47.

<sup>220</sup> 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 persoonsgegeven.



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.”<sup>221</sup>

Een persoon is identificeerbaar indien zijn identiteit - direct of via nadere stappen, door gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor zijn persoon<sup>222</sup> - redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.<sup>223</sup> 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.<sup>224</sup> Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke.<sup>225</sup> In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.<sup>226</sup>

### Beoordeling

Het CBP heeft in paragrafen 2.4 tot en met 2.7 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone in verschillende apparatuur en systemen (onder andere afhankelijk van de websites die zij bezoeken of apps en protocollen die zij gebruik(t)en) combinaties van de gegevens over en uit het dataverkeer van abonnees van haar dataverkeersdiensten (betrokkenen) verwerkt(e) als beschreven in **bijlage II** bij dit rapport.

---

<sup>221</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 47.

<sup>222</sup> 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.

<sup>223</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip ‘onevenredige inspanning’ opgemerkt: “Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen.” Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.

<sup>224</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 48. Vgl. ook WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 16. Daarbij moet rekening worden gehouden met alle relevante factoren, zoals de kosten van identificatie, het beoogde doel van de verwerking, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico op organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 16.

<sup>225</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 48-49.

<sup>226</sup> Idem, p. 49. Registratiekamer 27 maart 1995, 95.V.029.

Daarbij beschikt Vodafone over de NAW-gegevens en/of e-mailadressen van (een groot deel van) haar abonnees<sup>227</sup>, op grond van hun contractuele relatie, en in sommige gevallen over locatiegegevens.

Het CBP heeft in paragrafen 2.4 tot en met 2.7 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone de hierboven genoemde gegevens over en uit het dataverkeer verzamelt, gebruikt (en voor de doeleinden verkeersbeheer, beveiliging en de behandeling van verzoeken om inlichtingen van klanten vastlegt en bewaart op persoonsniveau, althans geaggregeerd per abonnee). Dit doet zij om het data ge-/verbruik en netwerkgebruik van betrokkenen in kaart te brengen.

#### *Gegevens 'betreffende' een persoon*

Het MSISDN, IMSI-klantnummer en het IMEI-toestelnummer (unieke klant- of toestel identifiers), op zichzelf of in onderlinge combinatie of in samenhang met (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over zijn mobiele data ge-/verbruik).<sup>228</sup>

Daarnaast zijn unieke klant- en/of toestel identifier(s), in combinatie met (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene gegevens over een natuurlijke persoon. Vodafone kan deze gegevens aanwenden om de betrokkene op een bepaalde wijze te behandelen of het gedrag van die persoon te beïnvloeden, op een wijze die gevolgen heeft voor de rechten/belangen van de betrokkene. Daarbij valt bijvoorbeeld te denken aan het analyseren van de inhoud van (gedownload) bestanden en verzonden en ontvangen e-mails op spam-, virus- en malware-herkenningspatronen om spam/virussen/malware tegen te houden en te verwijderen, het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed of aan het analyseren van het dataverkeer om een verzoek om inlichtingen af te handelen (oftewel, het gebruik van de gegevens in individuele gevallen met betrekking tot abonnees om technische defecten of fouten in de overbrenging van communicatie op te sporen en te verhelpen). De gegevens worden dus door Vodafone gebruikt op een wijze die in het maatschappelijk verkeer de betrokkene raakt (handelingen van Vodafone als aanbieder van communicatiediensten aan haar eigen klanten zijn onderdeel van het maatschappelijk verkeer).

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.<sup>229</sup>

---

<sup>227</sup> [VERTROUWELIJK] Reactie Vodafone op verzoek om inlichtingen van 11 april 2012.

<sup>228</sup> Hieruit volgt informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie.

<sup>229</sup> 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.cbpreweb.nl/Pages/pv\\_20110913\\_google.aspx](http://www.cbpreweb.nl/Pages/pv_20110913_google.aspx) (URL laatst bezocht op 29 mei 2013).

Niet doorslaggevend is of Vodafone 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<sup>230</sup>, en die mogelijkheid is aanwezig. Vodafone 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), contactgegevens (waaronder het MSISDN als unieke klantidentificatie, e-mailadres(sen) en/of NAW-gegevens), en in sommige gevallen (2G-)locatiegegevens.

#### *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 Vodafone direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).

#### **Postpaid abonnees**

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

Het MSISDN, het unieke IMSI-klantnummer<sup>231</sup> en het unieke IMEI-toestelnummer van een abonnee met een postpaid data abonnement zijn voor Vodafone identificerend omdat zij een koppeling(smogelijkheid) heeft tussen deze nummers, gecombineerd met NAW-gegevens en/of e-mailadres(sen). Er kan dus een relatie tussen de gegevens worden gelegd.

Vodafone beschikt verder over een koppeling(smogelijkheid) tussen de unieke klant-en/of toestel identificatie(s) en (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen dan wel (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene.<sup>232</sup>

Niet alleen beschikt Vodafone over de (in)direct identificerende gegevens over en uit het dataverkeer in haar databases/bestanden, ook heeft zij ter zake kundige technici in dienst (waaronder de eerder genoemde medewerkers; zie het kopje 'Verloop onderzoek', p. 10 e.v. van dit rapport) en beschikt zij over de benodigde technische faciliteiten (waaronder applicaties om de databases te bevragen en de technische mogelijkheid om gegevens te exporteren uit deze databases) om de gegevens aan elkaar te koppelen of zo nodig via tussenstappen te herleiden naar de betrokken abonnee. Hieruit blijkt dat de inspanning die Vodafone moet verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is.

---

<sup>230</sup> *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 47.

<sup>231</sup> Aan dit IMSI zijn alle gegevens van een abonnee gebonden, zoals NAW-gegevens, of de abonnee prepaid is of een abonnement heeft en of deze wel of niet in het buitenland mag bellen.

<sup>232</sup> Ook hier kan een relatie tussen de gegevens worden gelegd.

Vodafone schrijft in haar zienswijze 1 dat het CBP voorbij gaat *"aan het feit dat de meeste gegevens niet toegankelijk zijn voor Vodafone medewerkers, of anderen, en slechts worden gebruikt in het kader van doorvoer. Vodafone hanteert daartoe bovendien een strikt beveiligingsbeleid en controleert dat geen toegang is verkregen, of kan zijn, tot bepaalde gegevens. Vodafone's medewerkers worden daarnaast getraind op privacy- en beveiligingsaspecten. (...) Ook zijn veel gegevens slechts in geanonimiseerde of geaggregeerde vorm beschikbaar en dus om die reden geen persoonsgegevens."*<sup>233</sup>

Ten aanzien van de door Vodafone gehanteerde technische en organisatorische maatregelen, waaronder toegangsautorisaties (slechts een selecte groep medewerkers heeft toegang tot gebruik van de data analyse apparatuur), toegangsbeveiliging en controle daarop geldt dat dit bovenal een technische en organisatorische waarborg betreft ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp.<sup>234</sup> De omstandigheid dat slechts bepaalde medewerkers toegang hebben tot de data-analyse apparatuur en de data die met behulp daarvan wordt verwerkt, leidt echter niet tot de conclusie dat er geen sprake is van persoonsgegevens. De toegepaste aggregatie op abonnee-niveau (via de [VERTROUWELIJK: apparatuur]) is geen anonimisering<sup>235</sup> of gegevensvernietiging. Dit geldt ook voor de versleutelde [VERTROUWELIJK: identifiër] in de [VERTROUWELIJK] voor verkeersbeheer doeleinden. [VERTROUWELIJK]

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

- (i) verkeersbeheer en facturering, onder andere om op abonneeniveau inzicht te hebben/krijgen in de netwerkbelasting als gevolg van de toename van het gebruik van allerlei websites en apps, om *heavy users* te identificeren<sup>236</sup> en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed;
- (ii) spam-, virus- en malwarebestrijding in individuele gevallen; en
- (iii) behandeling van verzoeken om inlichtingen van klanten (inclusief klachten over video-optimalisatie).

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

In de opinie van de Artikel 29 Werkgroep, het onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders, over het begrip persoonsgegeven is in dat verband opgemerkt: *"In dergelijke gevallen waarin het doel van de verwerking impliceert dat personen worden geïdentificeerd, kan worden verondersteld dat de voor de verwerking*

---

<sup>233</sup> Zienswijze 1 Vodafone, p. 32 (doorgenummerde pagina's op de faxbrief).

<sup>234</sup> Naleving van het bepaalde in artikel 13 van de Wbp (beveiliging) valt buiten de scope van dit onderzoek.

<sup>235</sup> Anonimiseren wordt in de wetsgeschiedenis bij de Wbp gedefinieerd als *"een vorm van vernietigen van persoonsgegevens althans in de gevallen dat de verwijdering van de naam ook tot gevolg heeft dat de betrokkene niet meer kan worden herleid. Alleen in dit laatste geval pleegt te worden gesproken van «anonimiseren»."* Kamerstukken II 1999/2000, 25 892, nr. 92c, p. 13.

<sup>236</sup> Of Vodafone 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.

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.”<sup>237</sup> 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.<sup>238</sup>

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

#### **Prepaid abonnees**

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

Vodafone heeft verklaard dat zij NAW-gegevens en/of e-mailadressen heeft van [VERTROUWELIJK] van de prepaid abonnees die daadwerkelijk gebruik maken van mobiel internet (ruim een kwart van het totaal aantal prepaid abonnees).<sup>239</sup>

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

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.”*<sup>240</sup>

In haar zienswijze 1 stelt Vodafone dat er bij prepaid abonnementen geen sprake is van persoonsgegevens *“omdat er dan geen identificerende gegevens betreffende de abonnee beschikbaar zijn.”*<sup>241</sup>

Ten aanzien van de prepaid abonnees van wie Vodafone geen NAW-gegevens en/of e-mailadressen heeft, beschikt Vodafone wel over ten minste MSISDN (een direct

---

<sup>237</sup> WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 16-17.

<sup>238</sup> Idem, p. 22.

<sup>239</sup> Reactie Vodafone op verzoek om inlichtingen van 11 april 2012.

<sup>240</sup> *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 80.

<sup>241</sup> Zienswijze 1 Vodafone, p. 27 (doorgenummerde pagina's op de faxbrief).

contactgegevens door middel waarvan Vodafone met de abonnee in contact kan treden, om zijn identiteit vast te stellen), IMSI- en/of IMEI-nummer.

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).<sup>242</sup>

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.”*<sup>243</sup>

#### **Zakelijke abonnees**

Ook bedrijfsinformatie (bijvoorbeeld het 06-nummer en bedrijfs-e-mailadres van een zakelijke abonnee die normaliter wordt gebruikt door een specifieke werknemer) is in een aantal gevallen als persoonsgegevens te beschouwen, bijvoorbeeld omdat de naam van de werknemer binnen dat bedrijf wordt vastgelegd. Ook gegevens over eenmanszaken en bedrijven handelend onder een eigennaam worden als persoonsgegevens aangemerkt, wanneer die ook iets zeggen over het gedrag van de eigenaar.<sup>244</sup>

<sup>242</sup> WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 14-15.

<sup>243</sup> HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

<sup>244</sup> Vgl. ‘Klant in het web. Privacywaarborgen voor internettoegang’, A&V-studie nr. 17, Registratiekamer juni 2000, p. 34 en 58. URL: [http://www.cbppweb.nl/downloads\\_av/av17.pdf](http://www.cbppweb.nl/downloads_av/av17.pdf) (URL laatst bezocht op 29 mei 2013). Vgl. WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 25. In deze opinie is verder opgemerkt over identificeerbaarheid: *“In die context wordt door de voor de verwerking verantwoordelijken vaak aangevoerd dat identificatie slechts zal plaatsvinden voor een gering percentage van het verzamelde materiaal en dat er dus vóór de identificatie in die paar gevallen plaatsvindt, geen sprake is van verwerking van persoonsgegevens. Het doel van videobewaking is echter de identificatie van de personen die op de videobeelden te zien zijn, in alle gevallen dat de voor de verwerking verantwoordelijke dat nodig acht. Het hele proces moet dan ook worden beschouwd als de verwerking van gegevens over identificeerbare personen, ook als sommige personen in de praktijk niet identificeerbaar zijn.”* Idem, p. 17.

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

De persoonsgegevens (informatie) over het communicatiegedrag van betrokkenen zijn gegevens van gevoelige aard.<sup>245</sup>

#### **Verdere verwerking**

Vodafone verwerkt de persoonsgegevens verder door rapportages uit de [VERTROUWELIJK: apparatuur] te gebruiken voor het vaststellen van de business strategie van Vodafone. Het CBP heeft vastgesteld dat deze rapportages geaggregeerde *anonieme* gegevens bevatten die redelijkerwijs niet (meer) direct of indirect te herleiden zijn tot natuurlijke personen, niet door Vodafone of door enig ander persoon. Het zijn daarom in deze context geen persoonsgegevens in de zin van artikel 1, aanhef en onder a, van de Wbp.

### **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.

<sup>245</sup> 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](http://www.cbppweb.nl/downloads_int/wp185_en.pdf). Zie ook Definitieve bevindingen Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google van 7 december 2010 (z2010-00582), p. 34 e.v. Zie Bevindingen Onderzoek door het College bescherming persoonsgegevens (CBP) naar de verwerking van persoonsgegevens door Advance Concepts B.V. van 15 december 2009, p. 27 en 28. URL: [http://cbppweb.nl/downloads\\_pb/pb\\_20091218\\_advance\\_bevindingen.pdf](http://cbppweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf) (URL's laatst bezocht op 29 mei 2013).

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.”*<sup>246</sup>

Overweging 15 van de e-Privacyrichtlijn luidt:

*“Een communicatie kan naamgevings-, nummerings- of adresseringsgegevens omvatten die door de verzender van een communicatie of door de gebruiker van een verbinding worden verstrekt om de communicatie tot stand te brengen. Wanneer deze gegevens door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren zij ook tot de verkeersgegevens. Verkeersgegevens kunnen o.a. gegevens zijn met betrekking tot de routing, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop communicatie begint of eindigt, het begin, het einde of de duur van de verbinding (...).”*<sup>247</sup>

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

Of sprake is van persoonsgegevens die verkeersgegevens zijn, is afhankelijk van het doel van de verwerking, te weten: voor het overbrengen van communicatie of voor andere doelen.<sup>248</sup>

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*

---

<sup>246</sup> 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.).

<sup>247</sup> 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.

<sup>248</sup> W.A.M. Steenbruggen, ‘Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?’, *Computerrecht* 2003, p. 28.



*hebben het recht heeft op een zorgvuldige omgang met zijn gegevens, alsmede het recht op bescherming van zijn persoonlijke levenssfeer.”*<sup>249</sup>

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

Zowel de inhoud van, als informatie over elektronische communicatie<sup>250</sup> zijn gegevens die ook bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest).<sup>251</sup> Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) oordeelde in zijn arrest van 3 april 2007 over de bescherming van e-mailcorrespondentie en internetgebruik:

*“Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8”, (onderstreping toegevoegd door het CBP).*<sup>252</sup>

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.”<sup>253</sup>

---

<sup>249</sup> Kamerstukken II 2007/08, 31 145, nr. 9, p. 16-17.

<sup>250</sup> “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).

<sup>251</sup> De in artikel 7 van het Handvest gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Dit recht heeft dezelfde inhoud en reikwijdte als het recht in de daarmee corresponderende bepaling van het EVRM. Artikel 8 van het Handvest is een afzonderlijke bepaling over de bescherming van persoonsgegevens. Toelichtingen bij het Handvest van de grondrechten. URL: <http://eur-lex.europa.eu/nl/treaties/dat/32007X1214/htm/C2007303NL.01001701.htm> (URL laatst bezocht op 29 mei 2013). Het CBP heeft (daarom) in zijn wetgevingsadvies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet van 11 februari 2013 geadviseerd nadere aandacht te schenken aan de reikwijdte van het voorgestelde artikel 13 van de Grondwet (de uitzondering voor verkeersgegevens). URL: [http://www.cbpreweb.nl/Pages/adv\\_z2012-00746.aspx](http://www.cbpreweb.nl/Pages/adv_z2012-00746.aspx) (URL laatst bezocht op 29 mei 2013).

<sup>252</sup> EHRM 3 april 2007, NJ 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44.

<sup>253</sup> 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 (...).”

## 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 wetsgeschiedenis<sup>254</sup> geeft een indicatie welke categorieën van gegevens over en uit het dataverkeer als verkeersgegevens moeten worden aangemerkt. Beide noemen onder andere de routing, de duur, het tijdstip, het volume van de communicatie en het gebruikte protocol als gegevens die door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen.

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

De gegevens over het dataverkeer zijn (derhalve) zulke verkeersgegevens (die ook persoonsgegevens zijn), voor zover er daadwerkelijke communicatie plaatsvindt.<sup>255</sup> De verkeersgegevens over het communicatiegedrag van betrokkenen (bijvoorbeeld URL's) zijn gegevens van gevoelige aard.<sup>256</sup> 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

---

<sup>254</sup> 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.

<sup>255</sup> Voor zover ten aanzien van een toestel in stand-by stand (oftewel: *idle mode*) onder andere locatiegegevens worden verzonden over het signaleringskanaal om ervoor te zorgen dat het op elk moment inkomende berichten kan ontvangen, geldt dat geen sprake is van verkeersgegevens (alleen maar van persoonsgegevens) omdat er geen communicatie wordt/is gevoerd. Vgl. M.G.M. Hoegendijk, *Zakboek Strafvordering voor de Hulpofficier* 2011/9.14, p. 5; T&C *Strafvordering*, commentaar op artikel 126n Sv. De Hoge Raad heeft overwogen in zijn arrest van 7 september 2004: "(...) [onder inlichtingen ter zake van alle verkeer, oftewel verkeersgegevens, vallen, toevoeging door het CBP] gegevens betreffende de locatie van een gebruiker van een telecommunicatiemiddel, althans indien en voor zover deze het middel ook daadwerkelijk gebruikt en aan het telecommunicatieverkeer deelneemt." HR 7 september 2004, NJ 2004, 610. Gegevens die in idle mode over het signaleringskanaal worden verzonden vallen buiten de scope van dit onderzoek.

<sup>256</sup> *Kamerstukken II 2000/01*, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.

telecommunicatiegegevens is daarover opgemerkt: *“Op grond van de richtlijn moeten alleen de gegevens betreffende internettoegang bewaard worden en niet de gegevens over het websurfgedrag.”*<sup>257</sup> En: *“Het gaat niet om het opslaan van websites die zijn bezocht.”*<sup>258</sup> 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 (hierna: Dataretentierichtlijn). Artikel 1, tweede lid, van de Dataretentierichtlijn luidt: *“Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Zij is niet van toepassing op de inhoud van elektronische communicatie, de informatie die wordt geraadpleegd met behulp van een elektronisch communicatienetwerk daaronder begrepen.”* Artikel 5, tweede lid, van de Dataretentierichtlijn bepaalt: *“Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mogen krachtens deze richtlijn niet worden bewaard.”*

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

Deze kenmerken worden herkend in de initiatiefase van een protocol. In deze initiatiefase vindt nog geen overbrenging plaats van communicatie.

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

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

(Louter) gegevens uit het dataverkeer worden beoordeeld als communicatie, tevens persoonsgegevens. Ten aanzien van spam-, virus- en malwareherkenningsgegevens uit (gedownloade) bestanden en verzonden en ontvangen e-mails geldt, voor zover Vodafone deze verwerkt om spam en virussen/malware tegen te houden en te verwijderen, dat geen sprake is van verkeersgegevens, maar van zulke communicatie (de bestanden en berichten die worden overgebracht).<sup>259</sup>

<sup>257</sup> *Kamerstukken I* 2008/09, 31 145, C, p. 17. Zie in dezelfde zin idem, p. 12.

<sup>258</sup> *Handelingen II* 2007/08, 83, p. 5836.

<sup>259</sup> Het CBP heeft bovenstaande toepassing van de begrippen “communicatie” en “verkeersgegevens” voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom-CBP van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van deze begrippen in dit rapport.

Samengevat, kunnen de persoonsgegevens worden ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het 06-nummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume, IP-adres van-naar met poortnummer/protocol, URL's 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.<sup>260</sup> Ook het genereren van persoonsgegevens is een verwerking.<sup>261</sup> Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze gegevens.<sup>262</sup> 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).<sup>263</sup> Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen (*mere conduit*), verwerkt daarmee geen persoonsgegevens.<sup>264</sup>

#### **Beoordeling**

Het CBP heeft in paragrafen 2.4 tot en met 2.7 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone 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). Vodafone verwerkt (aldus) persoonsgegevens die (in de meeste gevallen) ook verkeersgegevens zijn. Er is geen sprake van een *mere conduit*-uitzondering.

Ofwel Vodafone verkrijgt (verzamelt) de persoonsgegevens via het gebruik van data-analyse technieken. Zo inspecteert Vodafone voor verkeersbeheer headergegevens in

---

<sup>260</sup> Zie *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 51-52.

<sup>261</sup> *Idem*, p. 51

<sup>262</sup> 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.

<sup>263</sup> Met dien verstande dat de desbetreffende handelingen met betrekking tot verkeersgegevens van abonnees die geen natuurlijke personen zijn niet zonder meer persoonsgegevens zijn.

<sup>264</sup> *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 68: “Zodra er enige feitelijke macht over persoonsgegevens is, is het wetsvoorstel van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking kunnen onder de wettelijke regeling vallen. Cruciaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige) invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend. Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing”, (onderstreping toegevoegd door het CBP). *Idem*, p. 51-52.

een datapakket dat van het toestel van de abonnee naar de applicatieserver gaat, (ii) voor het faciliteren van opwaardeermogelijkheden URL's om de (gratis) opwaardeersites te herkennen, (iii) voor spam-, virus- en malwarebestrijding (gedownload) bestanden en verzonden en ontvangen e-mails om spam/virussen/malware tegen te houden en te verwijderen en (iv) voor de behandeling van verzoeken om inlichtingen van klanten het dataverkeer op bijvoorbeeld (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan (ordering van al aanwezige gegevens).<sup>265</sup> Ofwel Vodafone analyseert/analyseerde via het gebruik van data-analyse technieken persoonsgegevens die worden aangemaakt in haar mobiele netwerk (bijvoorbeeld dataverbruik gegevens om te kunnen factureren).

Gelet op het voorgaande verwerkt Vodafone persoonsgegevens als bedoeld in artikel 1, aanhef en onder b, van de Wbp

### 3.6 Grondslag

#### **Uitwerking van het wettelijk kader**

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

Artikel 5, eerste en tweede lid, van de e-Privacyrichtlijn bepaalt (kort gezegd), voor zover voor dit onderzoek van belang: de lidstaten verbieden het 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. 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.<sup>266</sup>

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;*

<sup>265</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 68.

<sup>266</sup> Kamerstukken I 2011/12, 32 549, E, p. 2.

- c. deze handelingen noodzakelijk zijn voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder, of
- d. deze handelingen noodzakelijk zijn ter uitvoering van een wettelijk voorschrift of rechterlijk bevel.

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

In de wetsgeschiedenis bij artikel 11.2a is opgemerkt over *Deep Packet Inspection*: “Artikel 11.2a Tw ziet op de vertrouwelijkheid van de communicatie die via internet of andere elektronische communicatiediensten of -netwerken plaats vindt. Dit artikel waarborgt aldus dat de vertrouwelijkheid van de communicatie van bedrijven en consumenten, bijvoorbeeld via internet, wordt gewaarborgd. Overigens verbiedt artikel 11.2a Tw in den brede het aftappen of afluisteren, en dergelijke van communicatie door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, dus ook wanneer dit plaats heeft met een andere methode dan de methode van Deep Packet Inspection. Bezien vanuit de positie van de aanbieders van elektronische communicatienetwerken en diensten stellen beide artikelen grenzen aan het beheer van de door hen aangeboden netwerken en diensten. Belangrijk op te merken is dat zowel artikel 7.4a als artikel 11.2a Tw (zie met name tweede lid, onder b en c) er niet aan in de weg staan dat een aanbieder zijn netwerk en diensten op een «normale» manier beheert. Zo mag, ook in het kader van artikel 11.2a Tw (zie tweede lid, onder c), een aanbieder van een netwerk om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is de diverse verkeersstromen die over dat netwerk worden afgewikkeld in kaart brengen. Hij mag in dat kader, bijvoorbeeld, gegevens verzamelen over het volume van het verkeer van bepaalde diensten of applicaties, het aantal keren dat verbinding wordt gemaakt et cetera. Wel is belangrijk dat het verzamelen van dergelijke gegevens niet verder gaat dan nodig is voor het goed laten functioneren van het netwerk en de daarover afgewikkelde diensten. Ook laten beide artikelen toe dat maatregelen worden genomen ter voorkoming van congestie. Zo staat artikel 11.2a Tw (zie het tweede lid, onder c) noch artikel 7.4a Tw er aan in de weg dat een aanbieder kijkt of hij te maken heeft met een VOIP dienst of een e-mail dienst om deze vervolgens om voor de hand liggende redenen (pakketverlies maakt een e-mail onleesbaar maar enige vertraging is geen probleem, bij VOIP verkeer is dit juist andersom) bij congestie verschillend te behandelen”, (onderstreeping toegevoegd door het CBP).<sup>267</sup>

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,

<sup>267</sup> Idem, p. 13.

*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.”<sup>268</sup>*

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.”<sup>269</sup>*

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.*

<sup>268</sup> Kamerstukken I 2011/12, 32 549, F, p. 5.

<sup>269</sup> Kamerstukken II 2010/11, 32 549, nr. 16, p. 2-3.

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

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

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

b. de levering van diensten met toegevoegde waarde, mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor voorafgaand aan de verwerking zijn toestemming heeft gegeven. (...) <sup>270</sup>

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

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

#### Overbrenging van communicatie

De hoofdregel uit artikel 11.5 van de Tw is dat alle door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees en gebruikers worden verwijderd dan wel geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. <sup>271</sup> Voor dataverkeer is dit bijvoorbeeld afhankelijk van het type dienst. <sup>272</sup>

Onder het begrip ‘anonimiseren’ wordt verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken. <sup>273</sup> De gegevens moeten zodanig worden bewerkt dat ze redelijkerwijs niet

<sup>270</sup> 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.

<sup>271</sup> *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 154.

<sup>272</sup> *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.

<sup>273</sup> *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 80.



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.<sup>274</sup> 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).<sup>275</sup> In de wetsgeschiedenis bij de Tw wordt daarover opgemerkt: “Daarmee komt ook buiten kijf te staan dat de verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed; dit laatste dient onder facturering te worden begrepen.”<sup>276</sup>

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).<sup>277</sup> Het gaat hier niet om zelfstandige verwerkingsdoelen, maar om verwerkingsdoelen die van het factureringsdoel en het overbrengen van de communicatie zijn afgeleid.<sup>278</sup> De verkeersgegevens mogen (ook) voor die (afgeleide) doelen worden verwerkt, voor zover noodzakelijk.

<sup>274</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 48.

<sup>275</sup> Kamerstukken II 2002/03, 28 851, nr. 3, p. 155.

<sup>276</sup> Idem, nr. 13, p. 20.

<sup>277</sup> Idem, nr. 3, p. 156.

<sup>278</sup> Idem.

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

Het EHRM overweegt in zijn arrest van 25 maart 1983 over het begrip noodzakelijk: *"(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (...)." <sup>279</sup>*

Het Hof van Justitie van de EG vult het begrip noodzakelijkheid, 'een autonoom begrip van gemeenschapsrecht', op een strikte wijze in.<sup>280</sup> Uit een arrest van het Hof van Justitie van de EG van 16 december 2008 volgt dat indien het (enige) doel de vergaring van statistische gegevens is, het niet noodzakelijk is de (persoons)gegevens op naam te bewaren en te verwerken.<sup>281</sup>

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.<sup>282</sup> Dit betekent niet dat in alle gevallen - ongeacht of er sprake is van wel of niet betaling of wel of niet betwisting van de factuur - de verkeersgegevens tot het einde van die termijn mogen worden bewaard. In de gevallen dat de factuur is betaald en er voor het overige daaromtrent geen geschillen ontstaan, is het niet nodig de desbetreffende verkeersgegevens langer voor dat doel te bewaren.<sup>283</sup>

#### **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).<sup>284</sup>

<sup>279</sup> EHRM 25 maart 1983, nr. 97 (Silver & Others v. United Kingdom).

<sup>280</sup> Vgl. ook HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 52.

<sup>281</sup> HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 64-65 en 68: *"Evenzo gaat verordening nr. 862/2007, die de verstrekking regelt van van statistische gegevens over de migratiebewegingen op het grondgebied van de lidstaten, ervan uit dat de lidstaten de informatie verzamelen op basis waarvan die statistieken kunnen worden opgesteld. De uitoefening van die bevoegdheid maakt echter niet het verzamelen en bewaren van gegevens op naam zoals plaatsvindt in het kader van een register als het AZR, noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46. Zoals de advocaat-generaal in punt 23 van zijn conclusie heeft aangegeven, is voor een dergelijk doel alleen de verwerking van anonieme gegevens noodzakelijk. (...) In geen geval kunnen als noodzakelijk in de zin van artikel 7, sub e, van richtlijn 95/46 worden beschouwd de bewaring en de verwerking van persoonsgegevens op naam in het kader van een register als het AZR, voor statistiekdoeleinden."* Vgl. AG HvJ 3 april 2008, zaak C-524/06 (Huber), r.o. 23: *"Statistieken zijn per definitie anoniem en niet persoonsgebonden."*

<sup>282</sup> Idem, p. 155. In veel gevallen zal dat neerkomen op een termijn van ten hoogste vijf jaar (artikel 3:307 e.v. van het Burgerlijk Wetboek).

<sup>283</sup> Idem.

<sup>284</sup> Het CBP heeft bovenstaande uitleg van artikel 11.5 van de Tw voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap OPENBARE VERSIE Rapport definitieve bevindingen 29 mei 2013

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.”*<sup>285</sup>

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

Artikel 8, aanhef en onder a, b, c en f, van de Wbp, bepaalt, voor zover voor dit onderzoek van belang: *persoonsgegevens mogen slechts worden verwerkt indien:*

- a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;*
- b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;*
- c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;*
- (...)*
- f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.*

Artikel 11.5 van de Tw geeft, voor zover voor dit onderzoek van belang, op dit punt een nadere begrenzing/inperking van de toegestane verwerkingen van verkeersgegevens, tevens persoonsgegevens in de sector elektronische communicatie.<sup>286</sup>

#### **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.<sup>287</sup> ‘Specifiek’ betekent dat de wilsuiking betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).<sup>288</sup> ‘Geïnformeerd’ betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.<sup>289</sup>

---

Telecom-CBP van beide toezichthouders. Agentschap Telecom stemt in met de voorgelegde toepassing van dit artikel in dit rapport.

<sup>285</sup> *Kamerstukken II 2002/03, 28 851, nr. 7, p. 54. Zie ook Kamerstukken II 2002/03, 28 851, nr. 3, p. 6.*

<sup>286</sup> 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.*

<sup>287</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.*

<sup>288</sup> *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*

OPENBARE VERSIE Rapport definitieve bevindingen 29 mei 2013 70

Van *ondubbelzinnige* toestemming is slechts sprake indien bij de verantwoordelijke elke twijfel is uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.<sup>290</sup> ‘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).<sup>291</sup> In de wetsgeschiedenis bij de Wbp is daarover opgemerkt:

*“Als voorbeeld noem ik algemene voorwaarden die van toepassing zijn op het sluiten van een overeenkomst. Indien in dergelijke voorwaarden wordt bepaald welke gegevens er voor welk doel en door wie verwerkt worden, wil dat nog niet automatisch zeggen dat betrokkene daartoe ondubbelzinnig zijn toestemming heeft gegeven, enkel omdat hij de betreffende overeenkomst heeft ondertekend.”*<sup>292</sup>

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.”*<sup>293</sup>

#### **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.<sup>294</sup> Daarbij geldt als voorwaarde dat het moet gaan om een overeenkomst waarbij de betrokkene partij is<sup>295</sup> en waarvan de gegevensverwerking een noodzakelijk uitvloeisel is (dat wil zeggen: als de overeenkomst niet goed kan worden uitgevoerd zonder de persoonsgegevens).<sup>296</sup>

---

*verwerking niet in de algemene voorwaarden moet worden opgenomen, maar in een aparte toestemmingsclausule.”* WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 40. URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187\\_nl.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_nl.pdf) (URL laatst bezocht op 29 mei 2013).

<sup>289</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.

<sup>290</sup> Idem, p. 80.

<sup>291</sup> 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.

<sup>292</sup> *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.

<sup>293</sup> WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 41.

<sup>294</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 80.

<sup>295</sup> 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.

<sup>296</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 81.

De uitgever van een krant mag bijvoorbeeld de persoonsgegevens van zijn abonnees verwerken omdat dat noodzakelijk is om de krant te kunnen bezorgen<sup>297</sup> (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).<sup>298</sup> De grondslag is strikt beperkt tot de gegevens die voor de uitvoering van de overeenkomst noodzakelijk zijn.

Als aanvullende, niet-essentiële gegevens worden verwerkt is deze grondslag niet van toepassing. Anders gezegd: er moet een rechtvaardiging voor de verwerking aanwezig zijn *in de relatie tot de specifieke individuele betrokkene*.<sup>299</sup> 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.<sup>300</sup> 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).<sup>301</sup> Anders gezegd: er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.<sup>302</sup> Daarbij moet onder andere worden gelet op de aard van de in het geding zijnde taak en de aard van

---

<sup>297</sup> *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).

<sup>298</sup> Zie ook HR 9 september 2011, L/JN 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).

<sup>299</sup> 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."

<sup>300</sup> 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.

<sup>301</sup> Idem, p. 82-83. Een verwerking die uitsluitend dient ter uitvoering van een wettelijk recht valt hier buiten.

<sup>302</sup> Idem, p. 82.

de betrokken persoonsgegevens.<sup>303</sup> 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.<sup>304</sup> 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.<sup>305</sup>

#### **Gerechtvaardigd belang**

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

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke (bijvoorbeeld om zijn reguliere bedrijfsactiviteiten te kunnen verrichten<sup>306</sup>) of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert. Deze grondslag kan worden toegepast indien de verwerking noodzakelijk is (proportionaliteitstoets: de inbreuk op de belangen van de bij de verwerking betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel) en het doeleinde kan niet anderszins of met minder ingrijpende middelen worden bereikt (subsidiariteitstoets).<sup>307</sup>

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.<sup>308</sup> 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.<sup>309</sup>

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.”*<sup>310</sup>

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

---

<sup>303</sup> Idem, p. 83.

<sup>304</sup> Idem.

<sup>305</sup> Idem.

<sup>306</sup> Idem, p. 86.

<sup>307</sup> 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.

<sup>308</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.*

<sup>309</sup> Idem.

<sup>310</sup> *Kamerstukken II 1998/99, 25 892, nr. 13, p. 5-6.*

deze gegevens niet langer nodig/noodzakelijk zijn ten behoeve van (het doel van) de overbrenging van communicatie (proportionaliteitstoets). Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor facturering, of voor marktonderzoek/verkoopactiviteiten en toegevoegde waardediensten mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor toestemming heeft gegeven).<sup>311</sup>

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp<sup>312</sup> op het punt van de bevoegdheid tot (toelaatbaarheid van) het bewaren van persoonsgegevens die ook verkeersgegevens zijn (oftewel, een verplichting tot verwijdering dan wel anonimisering van gegevens, met uitzonderingen).<sup>313</sup> 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).<sup>314</sup> Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) verwerkingsdoelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp.

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

---

<sup>311</sup> Onder 'overbrenging van communicatie' en 'facturering' moet ook verkeersbeheer, behandeling van verzoeken om inlichtingen van abonnees en opsporing van fraude worden begrepen (artikel 11.5, vijfde lid, van de Tw). De verkeersgegevens mogen (ook) voor die (afgeleide) verwerkingsdoelen worden verwerkt, voor zover noodzakelijk.

<sup>312</sup> Te weten: het vereiste dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

<sup>313</sup> *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.

<sup>314</sup> 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.

gegevensverwerking is toegestaan onder artikel 11.5 van de Tw ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de Tw ook geen grondslag is te vinden in de Wbp.

*Persoonsgegevens die ook communicatie betreffen*

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

Artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) geeft een verplichting voor de aanbieder van een openbare elektronische communicatiedienst en -netwerk om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Dit artikel 11.3 van de Tw stelt eisen aan de beveiliging van persoonsgegevens en geeft aldus een telecomspecifieke uitwerking van artikel 13 van de Wbp.<sup>315</sup> Het artikel geeft (dus) geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

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

Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.3 en/of artikel 11.2a van de Tw genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Dat daargelaten, geeft de regeling in artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en (richtlijnconforme uitleg van)<sup>316</sup> 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

---

<sup>315</sup> 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.

<sup>316</sup> 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*).



(geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp. Materieel (inhoudelijk) betekent dat als de gegevensverwerking is toegestaan onder artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw; dat wil zeggen: uit dit artikel een wettelijke plicht voortvloeit) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw; dat wil zeggen: uit dit artikel een verwerkings-/uitzonderingsgrond voortvloeit) ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw ook geen grondslag is te vinden in de Wbp (waarbij dit laatste artikel 8 van de Wbp in de toets materieel (inhoudelijk) dan enkel zijdelings een rol speelt).

## Beoordeling

### 3.6.1 Verkeersbeheer

#### Netwerkplanning

[VERTROUWELIJK]

Het CBP heeft in paragraaf 2.4 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone unieke klant- en toestelidentifiers in combinatie met gegevens over het bezoek aan en gebruik van apps, websites en protocollen inspecteert/genereert, gebruikt, vastlegt en gedurende zeven dagen bewaart voor netwerkplanning, om op een geaggregeerd niveau inzicht te krijgen in het dataverbruik op het netwerk (bijvoorbeeld percentage VOIP, videostreaming, messaging etc.).

Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Vodafone stelt in haar zienswijzen dat zij zich voor netwerkplanning baseert op het ruime verwerkingsdoel facturering, waaronder tevens verkeersbeheer dient te worden geschaard (artikel 11.5, vijfde jo. tweede lid, van de Tw).<sup>317</sup> Vodafone voegde daar in haar zienswijze 1 aan toe dat zij anticipeerde op de inwerkingtreding van de wijziging van de Tw, waarin specifieke voorschriften zijn opgenomen over het gebruik van data-analyse technieken.<sup>318</sup>

Als hoofdregel geldt op grond van artikel 5 van de e-Privacyrichtlijn (vanaf 1 januari 2013 geïmplementeerd in artikel 11.2a van de Tw) dat het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie én de

---

<sup>317</sup> Zie o.a. Zienswijze 1 Vodafone, p. 17 (doorgenummerde pagina's faxbrief).

<sup>318</sup> Idem, p. 31-32 (doorgenummerde pagina's faxbrief): "(...) In de tweede plaats is van belang dat het CBP op geen enkele wijze rekening houdt met de aanstaande wijziging van de Telecommunicatiewet, waarin (naar mag worden aangenomen) specifieke voorschriften zullen worden opgenomen over het gebruik van data-analyse technieken (alsmede het vereiste van netneutraliteit), in respectievelijk artikel 7.4a en 11.2a Tw.[voetnoten weggelaten door het CBP] Hoewel het wetsvoorstel waarin deze artikelen is opgenomen nog bij de Eerste Kamer ligt, anticipeert Vodafone op de inwerkingtreding van deze artikelen. (...) Om het netwerk en de diensten op een 'normale manier' te beheren mag de aanbieder in het kader van artikel 11.2a lid 2 sub c Tw gegevens verzamelen over het volume van het verkeer van bepaalde diensten of applicaties, het aantal keren dat verbinding wordt gemaakt, voor zover deze niet verder gaan dan nodig. De wijze waarop Vodafone haar data-analyse technieken thans hanteert voldoet aan de wetswijziging."

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*, 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.<sup>319</sup>

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

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

---

<sup>319</sup> Vgl. o.a. *Kamerstukken I* 2011/12, 32 549, E, p. 13 over het in kaart brengen van de diverse verkeersstromen die over dat netwerk worden afgewikkeld om te beoordelen of zijn netwerk goed is gedimensioneerd of dat wellicht uitbreiding nodig is.

die voor Vodafone 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.

Vodafone heeft aannemelijk gemaakt dat zij voor netwerkplanning trends moet kunnen onderkennen, bijvoorbeeld om op tijd knelpunten in het netwerk te herkennen, zodat ze eventueel de netwerkcapaciteit kan uitbreiden.<sup>320</sup> Om zulke trends te berekenen is statistische analyse nodig.

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

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

Het CBP wijst - nu de door Vodafone voor netwerkplanning verwerkte gegevens in feite worden gebruikt voor kwantitatief statistisch onderzoek - verder op een arrest van het Hof van Justitie van de EG van 16 december 2008, waaruit volgt dat indien het (enige) doel de vergaring van statistische gegevens is, het voor dat doeleinde niet noodzakelijk is om de gegevens op naam te bewaren en te verwerken.<sup>321</sup>

Er waren/zijn daarnaast meerdere mogelijkheden, en minder ingrijpende middelen, om hetzelfde resultaat te bereiken. Bijvoorbeeld, door (apparatuur die in staat is om) de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren in niet-persistent (werk)geheugen. Technische mogelijkheden in dat verband zijn onder andere (i) het (laten) aanpassen van de configuratie-instellingen op bestaande data-analyse apparatuur, zodat de gegevens/persoonsidentificerende kenmerken zo snel als mogelijk na het verzamelen worden verwijderd uit de verkregen dataset, (ii) het (doen) vervangen van bestaande data-analyse apparatuur door apparatuur die (wel) in staat is om de gegevens zo snel als mogelijk na het verzamelen onomkeerbaar te anonimiseren (in niet-persistent (werk)geheugen) of (iii) het (laten) toevoegen van een zogeheten privacy filter (al dan niet op een ander of afzonderlijk apparaat) om de gegevens zo snel als mogelijk na het verzamelen onomkeerbaar te anonimiseren.

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

---

<sup>320</sup> Zie o.a. Zienswijze 2 Vodafone, p. 26-27 en 30 en 56.

<sup>321</sup> HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber).

[VERTROUWELIJK] Een nieuw, voor Vodafone specifiek project om tot eventuele andere oplossingen te komen is volgens haar qua tijdsduur en projectkosten minstens van dezelfde omvang als [VERTROUWELIJK].

Het CBP neemt als het gaat om het maken van kosten door Vodafone (echter) ook mee in zijn beoordeling dat Vodafone mogelijk een beroep kan doen op de garantie in de contractsdocumentatie van de [VERTROUWELIJK: apparatuur] dat de producten en diensten voldoen aan de geldende wettelijke normen die op de leverancier en Vodafone rusten.<sup>322</sup>

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

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 eventueel oneigenlijk gebruik van de gegevens kan groot zijn.

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

Omdat Vodafone voor netwerkplanning via de [VERTROUWELIJK: apparatuur] de persoonsgegevens die ook verkeersgegevens zijn niet zo snel als mogelijk na het verzamelen verwijdert terwijl dat wel mogelijk is en was, kan het gedurende zeven dagen bewaren en verwerken van de gegevens in niet-geanonimiseerde vorm niet als noodzakelijk worden beschouwd. Doordat de verwerking niet proportioneel en niet subsidiair is voor verkeersbeheer en omdat Vodafone ook geen ander noodzakelijk verwerkingsdoel heeft voor de onder dit kopje besproken gegevensverwerking, handelt Vodafone in strijd met artikel 11.5 van de Tw. Hierdoor kan van een

---

<sup>322</sup> [VERTROUWELIJK]

grondslag als genoemd in artikel 8 van de Wbp evenmin sprake zijn en handelt Vodafone tevens in strijd met artikel 8 van de Wbp.

Vodafone heeft het CBP, na het sluiten van het onderzoek, medegedeeld dat de [VERTROUWELIJK: apparatuur] sinds vorig jaar niet meer in gebruik is, omdat [VERTROUWELIJK].<sup>323</sup> Het CBP heeft dit niet nader onderzocht. Voor zover vanaf dat moment van gegevensverwerking geen sprake meer is geweest, zijn de geconstateerde overtredingen op dit punt beëindigd.

[VERTROUWELIJK]

Het CBP heeft in paragraaf 2.4 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone unieke klant- en toestelidentifiers in combinatie met gegevens over het bezoek aan en gebruik van apps, websites en protocollen inspecteert/genereert en gebruikt voor netwerkplanning, om op geaggregeerd en geanonimiseerd niveau inzicht te krijgen in het gedrag van groepen klanten zoals de top10 van meest bezochte websites en meest gebruikte toestellen.

Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Vodafone stelt in haar zienswijzen dat zij zich voor netwerkplanning baseert op het verwerkingsdoel verkeersbeheer.<sup>324</sup>

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

Vodafone heeft (verder) aannemelijk gemaakt dat zij voor netwerkplanning trends moet kunnen onderkennen, bijvoorbeeld om op tijd knelpunten in het netwerk te herkennen, zodat ze eventueel de netwerkcapaciteit kan uitbreiden'.<sup>325</sup>

Nu de persoonsgegevens die ook verkeersgegevens zijn al na een uur na het verzamelen daarvan zijn vernietigd/geanonimiseerd en gedurende dit uur [VERTROUWELIJK] niet toegankelijk zijn voor Vodafone medewerkers, terwijl Vodafone in haar zienswijze 2 aannemelijk heeft gemaakt dat de [VERTROUWELIJK: apparatuur] die zij inzet voor netwerkplanning gegevens niet eerder kan anonimiseren zonder bijvoorbeeld een geheel nieuw product te (laten) ontwikkelen (wat kostbaar is)<sup>326</sup>, voldoet de verwerking voor netwerkplanning via de [VERTROUWELIJK: apparatuur] in deze specifieke context aan het proportionaliteits- en subsidiariteitsvereiste. Het CBP constateert ten aanzien van de onder dit kopje

<sup>323</sup> Brief Vodafone van 13 juni 2013.

<sup>324</sup> Zienswijze 2 Vodafone, p. 61. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 17.

<sup>325</sup> Zie o.a. Zienswijze 2 Vodafone, p. 26-27 en 30 en 56.

<sup>326</sup> Zie o.a. idem, p. 9-10, 55-57 en 65. Reactie Vodafone op vordering van 21 februari 2013, p. 9. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 10.

besproken gegevensverwerking op basis van het beschikbare onderzoeksmateriaal geen overtreding van artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

### *Netwerkmonitoring*

#### *[VERTROUWELIJK]*

Het CBP heeft in paragraaf 2.4 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone unieke klant- en toestelidentifiers in combinatie met (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan (gegevens zoals datavolume en al dan niet geslaagde connecties) inspecteerde/genereerde, gebruikte, vastlegde en bij aanvang van het onderzoek op verschillende aggregatieniveaus (vijftien minuten-, dag-, week- en maandbasis) gedurende respectievelijk zeven dagen, negentig dagen, één jaar en twee jaar bewaarde, voor netwerkmonitoring (het detecteren en oplossen van problemen in het netwerk).

Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Vodafone stelt in haar zienswijzen dat zij zich voor het detecteren en oplossen van problemen in het netwerk baseert op het ruime verwerkingsdoel facturering, waaronder tevens verkeersbeheer dient te worden geschaard (artikel 11.5, vijfde jo. tweede lid, van de Tw).<sup>327</sup>

Ten aanzien van het inspecteren/genereren (verzamelen) van de persoonsgegevens geldt dat er voor Vodafone een noodzaak is om de gegevens op deze niet-geanonimiseerde wijze te verwerken om de benodigde informatie te hebben/(kunnen) krijgen over het functioneren van het netwerk/toestel bij het gebruik daarvan. Vodafone heeft aannemelijk gemaakt dat er, gegeven de huidige stand van de techniek, geen andere manieren en minder ingrijpende middelen beschikbaar waren/zijn om hetzelfde resultaat te bereiken.

De noodzaak om gegevens over het dataverkeer te *verzamelen* behelst niet (zonder meer) een noodzaak om de aldus verkregen gegevens vervolgens ook op persoonsniveau te gebruiken, vast te leggen en te bewaren. Getoetst moet worden of ook die verwerking voldoet aan het proportionaliteits- en subsidiariteitsvereiste. De aard van de verzamelde persoonsgegevens, de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor gegevensvergaring in de vorm van data-analyse technieken naar aanleiding van het gebruik van het netwerk van de aanbieder) en het risico (kans x impact) voor de betrokkenen van verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, spelen een rol in de belangenafweging. Daarnaast worden de inspanning en kosten die voor Vodafone gepaard gaan met de ontwikkeling en implementatie van een alternatieve oplossing meegewogen, evenals de consequenties voor de continuïteit en integriteit van haar netwerk.

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

---

<sup>327</sup> Zie o.a. Zienswijze 1 Vodafone, p. 17 (doorgenummerde pagina's faxbrief).

de gegevensverwerking niet automatisch ook noodzakelijk en daarmee gerechtvaardigd.

Vodafone stelt zich meer in algemene zin op het standpunt dat het voor het detecteren en oplossen van problemen in het netwerk noodzakelijk is om gegevens op individueel niveau te verwerken, om storingen tijdig te kunnen oplossen.<sup>328</sup> Vodafone heeft dit in haar zienswijze 2 (nader) toegelicht aan de hand van een aantal voorbeelden die uiteenvallen in grofweg vijf categorieën.

[VERTROUWELIJK]

Het CBP neemt in aanmerking dat deze voorbeelden situaties representeren waarin Vodafone vooral op relatief korte termijn actie zal (moeten kunnen) ondernemen: het monitoren van incidenten en het managen daarvan.

Daarnaast heeft Vodafone aangegeven dat [VERTROUWELIJK].<sup>329</sup>

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

Vodafone lijkt ook te aanvaarden dat een alternatief op dit moment proportioneel is: zij heeft de bewaartermijnen van de persoonsgegevens wat betreft de verschillende aggregatieniveaus naar aanleiding van het onderzoek teruggebracht naar respectievelijk twee dagen, twee weken, tien weken en zes maanden (zie het kopje 'Getroffen maatregelen' hieronder).

Het gaat bovendien om de verwerking van verkeersgegevens die veel over de gebruiker kunnen zeggen (te weten: datagebruik met betrekking tot websites waarmee problemen bestaan, [VERTROUWELIJK]) en raken aan de telecommunicatievrijheid.

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

---

<sup>328</sup> Zie o.a. Zienswijze 2 Vodafone, p. 28 en Zienswijze 1 Vodafone, p. 28 (doorgenummerde pagina's faxbrief).

<sup>329</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 14 en Zienswijze 1 Vodafone, p. 26 (doorgenummerde pagina's faxbrief).

### **Getroffen maatregelen**

Vodafone heeft de bewaartermijnen van de persoonsgegevens die ook verkeersgegevens zijn wat betreft de verschillende aggregatieniveaus verkort tot respectievelijk twee dagen, twee weken, tien weken en zes maanden (zie paragraaf 2.4, p. 32 van dit rapport, onder het kopje 'Getroffen maatregelen').

Het CBP oordeelt dat Vodafone in de meeste gevallen aannemelijk heeft gemaakt dat de inzet van de [VERTROUWELIJK: apparatuur] in deze nieuwe configuratie noodzakelijk is voor de stabiliteit en integriteit van het netwerk alsmede de nakoming van bestaande overeenkomsten.

Alleen ten aanzien van het [VERTROUWELIJK: identifier] ontbreekt een noodzaak om het volledige nummer zes maanden te bewaren. [VERTROUWELIJK] Vodafone geeft aan de [VERTROUWELIJK: identifier] nodig te hebben om problemen te herkennen in verband met OS-updates.

Vodafone heeft niet gesteld en niet is gebleken dat Vodafone voor dit doel de betrokkenen moet kunnen bereiken of onderscheiden.

Gelet daarop is niet aannemelijk geworden dat Vodafone voor dat doel niet zou kunnen volstaan met het bewaren en verwerken van de [VERTROUWELIJK]. Dit in plaats van het volledige [VERTROUWELIJK: identifier], te bewaren en verwerken. Het [VERTROUWELIJK] brengt (de grootste) identificeerbaarheid mee, omdat het op zichzelf persoonsidentificerende kenmerken bevat, ook zonder de onderlinge combinatie of in samenhang met uit andere bron bekende informatie.

Omdat Vodafone voor netwerkmonitoring via de [VERTROUWELIJK: apparatuur] voor het signaleren van problemen in verband met OS-updates naar het oordeel van het CBP ook zou kunnen volstaan met het bewaren en verwerken van een gedeelte van het [VERTROUWELIJK: identifier] in plaats van het volledige nummer in de zes maanden geaggregeerde data, heeft zij geen grondslag voor de verwerking van het volledige [VERTROUWELIJK: identifier] voor het doeleinde verkeersbeheer, gedurende deze verwerkingsduur. Hierdoor handelt Vodafone ten aanzien van het [VERTROUWELIJK: identifier] (nog) in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Doordat Vodafone voor het detecteren en oplossen van problemen in het netwerk via de [VERTROUWELIJK: apparatuur] de persoonsgegevens wat betreft de overige aggregatieniveaus inmiddels zo snel als mogelijk na het verzamelen verwijdert, heeft zij in zoverre wel een grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Op deze punten handelt Vodafone niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

### ***Video-optimalisatie***

Het CBP heeft in paragraaf 2.4 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone gegevens over het dataverkeer van betrokkenen<sup>330</sup> genereert/verzamelt en gebruikt voor video-optimalisatie.

---

<sup>330</sup> [VERTROUWELIJK]



Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

Vodafone inspecteert en analyseert bij de toegepaste video-optimalisatie alle URL's van de video's om [VERTROUWELIJK] compressie op video's en webpagina's toe te kunnen passen, tijdens de internetssessie van een abonnee.

Vodafone licht in haar zienswijze 1 toe: *"Video-optimalisatie is in het belang van de eindgebruiker; als dit niet wordt geboden werkt het netwerk langzamer, zal het bekijken van videobeelden vaker vastlopen en is de klant bovendien duurder uit. (...) Redelijkerwijs valt dan ook niet in te zien waarom een klant tegen video-optimalisatie bezwaar zou kunnen hebben (...)." <sup>331</sup>*

Op grond van artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw is de verwerking van niet-geanonimiseerde verkeersgegevens toelaatbaar indien deze noodzakelijk is voor 'verkeersbeheer' (oftewel, activiteiten ter verbetering van de netwerk performance of de dienstverlening van de mobiele aanbieder). Vodafone heeft verklaard dat de verwerking van persoonsgegevens noodzakelijk is om bijvoorbeeld video's met de gewenste snelheid te kunnen leveren én om de abonnee geld te besparen voor onnodig dataverkeer.<sup>332</sup> Vodafone heeft aannemelijk gemaakt dat hieruit volgt dat de verwerking van de persoonsgegevens voor Vodafone noodzakelijk is om bijvoorbeeld haar reguliere bedrijfsactiviteiten te kunnen verrichten als aanbieder van een openbare elektronisch communicatienetwerk en -dienst. Uit het voorgaande blijkt dat Vodafone een beroep kan doen op het verwerkingsdoel verkeersbeheer (artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw). Zo'n verwerkingsdoel correspondeert met de grondslagen uitvoering van een overeenkomst en/of een noodzaak (artikel 8, aanhef en onder b en/of f, van de Wbp). Dit omdat als de gegevensverwerking is toegestaan onder artikel 11.5 van de Tw ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de Tw ook geen grondslag is te vinden in de Wbp.

Het CBP constateert ten aanzien van de onder dit kopje besproken gegevensverwerking op basis van het beschikbare onderzoeksmateriaal geen overtreding van artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

### **3.6.2 Facturering (prepaidverkeer)**

Het CBP heeft in paragraaf 2.5 (p. 37 e.v. van dit rapport) vastgesteld dat Vodafone (een) unieke klant- en/of toestelidentificatie(s) in combinatie met de URL inspecteert en gebruikt om daaruit gratis opwaardeersites te herkennen voor het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed.

Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook verkeersgegevens zijn.

---

<sup>331</sup> Zienswijze 1 Vodafone, p. 38 (doorgenummerde pagina's op de faxbrief).

<sup>332</sup> Idem.

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

Vodafone stelt in haar zienswijzen dat zij zich voor het routeren van verkeer naar opwaardeersites voor opwaardering baseert op het verwerkingsdoel facturering.<sup>333</sup>

Vodafone licht in haar zienswijze 2 toe dat de overeenkomst tussen haar en een eindgebruiker tot stand komt door ingebruikname van een prepaid sim-kaart en eindigt door een afsluiting van deze sim-kaart van het netwerk (artikel 4, eerste lid, van de Algemene Voorwaarden voor Consumenten). De overeenkomst eindigt niet als zijn tegoed op is. Surfen naar de opwaardeersite vindt plaats in een contractuele context: Vodafone biedt de mogelijkheid tot gratis opwaardering (aanbod) en zodra de gratis site wordt bezocht, wordt dat aanbod (dat wil zeggen: de mogelijkheid om gratis op te waarden) aanvaard.<sup>334</sup>

Vodafone betwist ook dat het faciliteren van toegang tot een gratis opwaardeersite naar zijn aard een verkoopactiviteit is waarvoor toestemming is vereist, nu dit valt onder een en hetzelfde contract dan wel het aanvaarding is van het aanbod om zonder meerkosten voor datagebruik het tegoed op te waarden. Los daarvan is het volgens Vodafone zo dat als deze redenering zou worden doorgetrokken zij steeds als de abonnee surft naar een site waar hij iets kan kopen, Vodafone dat alleen kan faciliteren als daarvoor toestemming wordt gegeven.<sup>335</sup>

Uit de wetsgeschiedenis bij de Tw volgt (inderdaad) dat het verwerkingsdoel facturering, genoemd in artikel 11.5, tweede lid, van de Tw, 'ruim' dient te worden opgevat in de zin dat verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed (dit laatste dient onder facturering te worden begrepen).<sup>336</sup> Dit verwerkingsdoel correspondeert met de grondslag uitvoering van een overeenkomst en - mogelijk - noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

De enkele omstandigheid dat onder de verwerking ten behoeve van de facturering niet alleen wordt verstaan het opstellen van een factuur, maar ook het afwaarderen van het prepaidtegoed bij gebruik van de prepaidaansluiting met de verschuldigde vergoedingen en het bijhouden van het tegoed (het betreft immers vooruitbetaald(e) kaarten/gebruiksrechten; als het prepaidtegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante dienst (nog) te gebruiken), maakt niet dat het bieden van de mogelijkheid om nieuw tegoed te kopen daar ook zonder meer onder valt. Het faciliteren van opwaardeermogelijkheden is in beginsel - naar zijn aard - veeleer een verkoopactiviteit in de zin van artikel 11.5, derde lid, van de Tw waarvoor toestemming is vereist (die bij opwaardering een

---

<sup>333</sup> Zienswijze 1 Vodafone, p. 40 (doorgenummerde pagina's op de faxbrief) en Zienswijze 2 Vodafone, p. 68.

<sup>334</sup> Zienswijze 2 Vodafone, p. 68-69.

<sup>335</sup> Idem, p. 70.

<sup>336</sup> *Kamerstukken II* 2002/03, 28 851, nr. 13, p. 20.

betalingsverplichting in het leven roept wat (wederom) noodzaakt tot het bijhouden van het tegoed).

Op grond van haar algemene voorwaarden 'Algemene Voorwaarden Consumenten Vodafone Libertel B.V.' wordt de prepaid-overeenkomst in principe gesloten voor onbepaalde duur: *"Is jouw tegoed verbruikt of verlopen, dan kun je nog maar beperkt gebruik maken van jouw prepaid-overeenkomst (zoals bijvoorbeeld bellen naar 112). Binnen een bepaalde termijn kun je nieuw tegoed kopen"*, (artikel 4, eerste lid). Het CBP volgt Vodafone in haar betoog dat surfen naar de opwaardeersite aldus plaatsvindt in een contractuele context, dan wel het aanvaarding is van het aanbod van Vodafone om zonder meerkosten voor datagebruik het tegoed (ook) via 'mobiel internet' op te waarderen (om te voorkomen dat de betrokken abonnee zijn prepaid tegoed alsdan alleen kan opwaarderen via bijvoorbeeld een andere, 'vaste' internetverbinding). Dit ook vanuit de grondgedachte dat een eindgebruiker binnen een bepaalde termijn nieuw tegoed moet kunnen kopen. Hieruit volgt dat de verwerking van gegevens om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor de facturering. Een abonnee verwacht dit ook.

Het CBP heeft deze uitleg van de wet, dat het faciliteren van opwaardeermogelijkheden op het eerste gezicht wellicht een verkoopactiviteit lijkt waarvoor toestemming is vereist, maar gelet op de contractuele context en vanuit de grondgedachte dat een eindgebruiker binnen een bepaalde termijn nieuw tegoed moet kunnen kopen noodzakelijk *kan* zijn voor het ruime verwerkingsdoel facturering (mits er een proportionele implementatie is), (nogmaals) voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom-CBP. Agentschap Telecom stemt in met deze voorgelegde toepassing van dit wetsartikel.

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

Hieruit volgt dat, gelet op de door Vodafone gekozen en gebruikte implementatie bij aanvang van het onderzoek, de verwerkte gegevens niet als noodzakelijk konden worden beschouwd.

Doordat de verwerking niet proportioneel en niet subsidiair was voor facturering en omdat Vodafone ook geen ander noodzakelijk verwerkingsdoel had voor de in deze paragraaf besproken gegevensverwerking, handelde Vodafone in strijd met artikel 11.5 van de Tw. Hierdoor kon van een grondslag als genoemd in artikel 8 van de Wbp evenmin sprake zijn en handelde Vodafone tevens in strijd met artikel 8 van de Wbp.

### **Getroffen maatregelen**

Vodafone verleent thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK]. Dit is in deze context een proportionele implementatie van het bieden van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed, direct via 'mobiel internet', gelet op de omstandigheid dat de verwerkte gegevens niet worden opgeslagen en bewaard. Door deze aanpassing handelt Vodafone niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

### **3.6.3 Firewalls, spamfilters en virusscanners**

Het CBP heeft in paragraaf 2.6 (p. 42 e.v. van dit rapport) vastgesteld dat Vodafone (een) unieke klant- en/of toestelidentificatie(s) in combinatie met spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer van betrokkenen genereert/verzamelt, gebruikt, vastlegt en de logfiles van opgespoorde anomalieën of beveiligingslekken gedurende ten hoogste twee maanden bewaart voor het (veilig) leveren van mobiel dataverkeer.

Het CBP heeft in paragraaf 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking is van persoonsgegevens die ook communicatie betreffen.

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

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

Artikel 11.3 van de Tw (de implementatie van artikel 4 van de e-Privacyrichtlijn) geeft een verplichting voor de aanbieder van een openbare elektronische communicatiedienst en -netwerk om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Onder de eisen die de zorgplicht internetveiligheid stelt, wordt onder andere begrepen het aanbieden van virusfilters voor inkomende en eventueel uitgaande e-mails en het bestrijden van spyware. Filtering van uitgaande spam kan naar het oordeel van het CBP ook noodzakelijk zijn voor Vodafone om deze wettelijke plicht uit te voeren.<sup>337</sup>

Het CBP heeft in paragraaf 2.6 (p. 42 e.v. van dit rapport) vastgesteld dat internet aanbieders ook naar de inhoud van (gedownload) bestanden en verzonden en ontvangen e-mails moeten kijken om spam/virussen/malware te kunnen herkennen.

<sup>337</sup> 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. Opinion 2/2006 on privacy issues related to the provision of email screening services van 21 februari 2006, p. 7. URL: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf) (URL laatst bezocht op 29 mei 2013).

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.<sup>338</sup>

Uit het voorgaande blijkt dat Vodafone een grondslag voor deze verwerking van persoonsgegevens die ook communicatie betreffen heeft onder artikel 11.3 van de Tw jo. artikel 8 van de Wbp. Op basis van het beschikbare onderzoeksmateriaal heeft het CBP ten aanzien van de in deze paragraaf besproken gegevensverwerking 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 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.”*<sup>339</sup>

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 ACM<sup>340</sup> 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.<sup>341</sup> De inzet van data-analyse technieken vanaf 1 januari 2013 voor het filteren op inkomende spam valt daarom buiten de scope van dit onderzoek.

---

<sup>338</sup> Vgl. ook idem, p. 5-7 over de zorgplicht van internet- en e-mailproviders.

<sup>339</sup> *Kamerstukken I 2011/12*, 32 549, G, p. 8.

<sup>340</sup> 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.

<sup>341</sup> Vgl. ook de taakverdeling ten aanzien van spam (artikel 5 van het Samenwerkingsprotocol CBP-OPTA).

### 3.6.4 Behandeling van verzoeken om inlichtingen van klanten

Het CBP heeft in paragraaf 2.7 (p. 44 van dit rapport) vastgesteld dat Vodafone gegevens over het dataverkeer van betrokkenen<sup>342</sup> verzamelt, gebruikt, vastlegt en bewaart om in specifieke, individuele gevallen inlichtingen te kunnen geven bij storingen en fouten. Het betreft gegevens over het dataverbruik en websites waarmee problemen bestaan.

Het CBP heeft in paragrafen 3.3 tot en met 3.5 (p. 50 e.v. van dit rapport) vastgesteld dat dit een verwerking van persoonsgegevens (tevens verkeersgegevens respectievelijk communicatie) is.

Vodafone heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming.<sup>343</sup> In haar zienswijze 1 voegt Vodafone toe dat ook uitvoering van de overeenkomst en, minst genomen, een gerechtvaardigd belang grondslagen van de verwerking vormen.<sup>344</sup>

#### *Persoonsgegevens die ook verkeersgegevens zijn*

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

Vodafone heeft als verzamel- en verwerkingsdoeleinde van de persoonsgegevens genoemd 'behandeling van verzoeken om inlichtingen van klanten. Om klachten en problemen van klanten op te lossen'. Uit het voorgaande blijkt dat Vodafone (daarom) een grondslag voor deze verwerking van persoonsgegevens die ook verkeersgegevens zijn zou kunnen hebben onder artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw. Zo'n verwerkingsdoel correspondeert met de grondslagen uitvoering van een overeenkomst en/of noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

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

#### *Persoonsgegevens die ook communicatie betreffen*

Voor zover Vodafone voor het doeleinde behandeling van verzoeken om inlichtingen van klanten ook persoonsgegevens die ook communicatie betreffen verwerkt, 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

---

<sup>342</sup> [VERTROUWELIJK]

<sup>343</sup> Zie Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>344</sup> Zienswijze 1 Vodafone, p. 39 (doorgenummerde pagina's op de faxbrief).

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

Vodafone heeft verklaard dat de verwerking van persoonsgegevens in individuele gevallen is gebaseerd op toestemming.<sup>345</sup> Van een geldige grondslag is (echter) slechts sprake indien deze toestemming 'voorafgaand' is.<sup>346</sup> Vodafone kan een wettelijke grondslag voor de verwerking ten behoeve van klachtbehandeling hebben, mits Vodafone betrokkenen om voorafgaande ondubbelzinnige toestemming zou vragen (dat wil zeggen: voorafgaand aan de gegevensverzameling) en die toestemming wordt verkregen. Dit is evenwel niet (nader) door het CBP onderzocht.

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

### 3.7 Verdere verwerking

Vodafone gebruikt de rapportages uit de [VERTROUWELIJK: apparatuur] voor het vaststellen van de business strategie van Vodafone.<sup>347</sup> Het CBP heeft vastgesteld dat deze rapportages geaggregeerde *anonieme* gegevens bevatten die redelijkerwijs niet (meer) direct of indirect te herleiden zijn tot natuurlijke personen, niet door Vodafone of door iemand anders. De Wbp is daarom niet (meer) van toepassing op deze verwerking (voor zover Vodafone op adequate wijze de risico's op heridentificatie minimaliseert).

---

<sup>345</sup> Zie Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>346</sup> Vgl. *Kamerstukken II 1998/99*, 25 892, nr. 9, p. 5 en URL: [http://www.cbppweb.nl/pages/med\\_20120514\\_televisieopnamen-vumc-strijdig-met-wbp.aspx](http://www.cbppweb.nl/pages/med_20120514_televisieopnamen-vumc-strijdig-met-wbp.aspx) (URL laatst bezocht op 29 mei 2013). Zie ook WP29 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 35-36 en 40: *"Het is verstandig om toestemming te verkrijgen voordat met de gegevensverwerking wordt begonnen. Als dat niet gebeurt, is het gedeelte van de verwerking dat heeft plaatsgevonden tussen de start van de verwerking en het moment dat de toestemming wordt verkregen onrechtmatig, omdat er geen wettelijke grond voor bestaat."*

<sup>347</sup> Reactie Vodafone op verzoek om inlichtingen van 24 oktober 2011, p. 1.

### 3.8 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.<sup>348</sup>

‘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).<sup>349</sup> Het doeleinde mag ook niet in de loop van het verzamelproces worden geformuleerd.<sup>350</sup> ‘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.<sup>351</sup>

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.”*<sup>352</sup>

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

#### **Beoordeling**

Het CBP heeft in paragraaf 2.4 tot en met 2.7 (p. 22 e.v. van dit rapport) vastgesteld dat Vodafone persoonsgegevens verzamelt/verwerkt bij de inzet van data-analyse technieken in haar mobiele netwerk.

#### *Uitdrukkelijk omschreven*

Vodafone heeft als doeleinden van de gegevensverwerking (samengevat weergegeven) geformuleerd, voor zover deze binnen de scope van dit onderzoek vallen: verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites), beveiliging (in het bijzonder spam-,

<sup>348</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 79.

<sup>349</sup> Idem.

<sup>350</sup> Idem.

<sup>351</sup> Idem.

<sup>352</sup> Idem.



virus- en malwarefiltering) en de behandeling van verzoeken om inlichtingen van klanten. Deze doeleinden zijn niet volledig en niet duidelijk omschreven in de doelomschrijving in de huidige melding die Vodafone heeft gedaan. De melding dat gegevens worden verwerkt voor de doeleinden 'het sluiten en uitvoeren van de overeenkomst die het gevolg is van de voornoemde aansluiting', 'het nakomen van de contractuele verplichtingen uit de overeenkomst', 'het voorkomen van fraude en misbruik en het bevorderen van de continuïteit en beveiliging van de Vodafone organisatie en het Vodafone netwerk' is te weinig specifiek. Het biedt bijvoorbeeld onvoldoende houvast om te kunnen voorzien dat Vodafone onder andere in kaart brengt welke capaciteit de soorten websites en applicaties die door haar klanten worden gebruikt, innemen om eventueel de netwerkcapaciteit kunnen uitbreiden, internetgegevens en informatie verwerkt over hoe het netwerk en de telefoon van een abonnee in combinatie met het netwerk werkt om storingen zo vroeg mogelijk in het netwerk te kunnen signaleren én video's in delen door het netwerk stuurt (zie p. 21 van dit rapport). De afweging van de belangen van de verantwoordelijke en de betrokkene is zodoende onvoldoende controleerbaar.<sup>353</sup>

Het CBP heeft in paragraaf 2.1 (p. 17 van dit rapport) vastgesteld dat Vodafone 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.<sup>354</sup> De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding.<sup>355</sup> Vodafone heeft geen eigen functionaris voor de 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).

---

<sup>353</sup> Idem, p. 132-133: "Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn."

<sup>354</sup> De enige artikelen die mogelijk anderszins in aanmerking zouden kunnen komen qua categorie(en) van vrijgestelde verwerking(en) zijn artikel 32 en 34 van het Vrijstellingsbesluit Wbp. Artikel 32 en 34 van het Vrijstellingsbesluit Wbp regelt slechts een vrijstelling van de melding voor verwerkingen in verband met het aanbieden van faciliteiten of diensten op een netwerk (niet zijnde een 'openbare elektronisch communicatienetwerk' of 'openbare elektronische communicatiediensten' als bedoeld in artikel 1.1, onder g en f, van de Tw) respectievelijk verwerkingen in verband met het gebruik van communicatieapparatuur die beschikbaar wordt gesteld 'aan personen die in dienst zijn van of werkzaam zijn ten behoeve van de verantwoordelijke', en dan nog alleen maar voor zover deze verwerkingen voldoen aan de in die artikelen vermelde eisen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens.

<sup>355</sup> 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."

Ten aanzien van de stelling van Vodafone in haar zienswijze 2 dat haar Privacy Statement een uitdrukkelijke omschrijving geeft van de doeleinden waarvoor zij persoonsgegevens verwerkt, neemt het CBP in aanmerking dat ofschoon blijkens de wetsgeschiedenis bij de vorm van de doelomschrijving lijkt te zijn gedacht aan de melding die zij op grond van artikel 27 jo. 28 van de Wbp (hierna: de meldingsplicht) verplicht is te doen<sup>356</sup>, de recente opinie van de Artikel 29-werkgroep over doelbinding ook ruimte laat voor de vorm van verwoording en uitdrukking van de doeleinden in een privacystatement ('notice'): *"Expressing the purposes under the meaning of Article 6(1)(b) may be accomplished in different ways. These include, for example, describing the purposes in a notice provided to the data subjects, in a notification provided to the supervisory authority, or internally in the information provided to a data protection officer. Some national laws specifically provide that both notices and notifications are acceptable forms of complying with the requirement of making the purposes of the processing explicit, but that they are not the only possibilities"*, (onderstreping toegevoegd door het CBP).<sup>357</sup>

In het oude Privacy Statement van Vodafone werd over het bijhouden van gegevens over het dataverkeer opgemerkt, voor zover voor dit onderzoek van belang: *"Zoals hiervoor al aangehaald verwerkt Vodafone ook uw bel- en/of internetgegevens. Vodafone kan bijhouden wanneer, hoe vaak, hoe lang even eventueel met wie/welke telefoonnummers u belt en/of verbinding heeft. (...) Ook ten behoeve van het verkeersbeheer voor het netwerk en voor gegevens-uitwisseling met telecombedrijven in het buitenland worden gegevens verwerkt"*, (onderstreping toegevoegd door het CBP).<sup>358</sup>

De doeleinden van de gegevensverwerking verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites), beveiliging (spam-, virus- en malwarefiltering) en de behandeling van verzoeken om inlichtingen van klanten waren ook onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving in het oude Privacy Statement. De betrokkene zal adequaat moeten worden geïnformeerd omtrent de concrete doelen van de gegevensverwerking.<sup>359</sup>

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

---

<sup>356</sup> Zie Kamerstukken II 1997/98, 25 892, nr. 3, p. 20 en 79: *"De omschrijving van het doel zal hetzij blijken uit de melding van de verwerking die de verantwoordelijke op grond van de wet uit hoofde van de wet verplicht is te verrichten – zie artikel 28, eerste lid, onder b, van het wetsvoorstel – hetzij uit de algemene maatregel van bestuur waarin precies zal worden geregeld welke verwerkingen van de meldingsverplichting worden vrijgesteld"* en *"Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen."*

<sup>357</sup> WP29 203. Opinion 03/2013 on purpose limitation van 2 april 2013, p. 18.

URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf) (URL laatst bezocht op 29 mei 2013).

<sup>358</sup> Privacy Statement Vodafone van september 2011.

<sup>359</sup> Kamerstukken II 1998/99, 25 892, nr. 6, p. 17.

#### *Gerechtvaardigd doeleinde*

Het CBP heeft in paragraaf X (p. X e.v. van dit rapport) vastgesteld dat Vodafone bij aanvang van het onderzoek niet in alle stadia van de verwerking een grondslag had voor de gegevensverwerkingen voor het doeleinde verkeersbeheer en facturering (meer in het bijzonder: netwerkplanning, netwerkmonitoring en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites).

Doordat de gegevensverwerking voor het doeleinde verkeersbeheer en facturering niet in alle stadia kon steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, werden de door Vodafone verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld en handelde Vodafone in strijd met artikel 7 van de Wbp.

#### **Voorgenomen en getroffen maatregelen**

Vodafone heeft bij haar zienswijze 1 onder meer een voorstel tot wijziging van de melding gevoegd.

In de concept gewijzigde melding wordt het doel van verwerking ‘sluiten en uitvoeren van de overeenkomst’ uitgebreid met een toelichting dat dit tevens factureren betreft, *“waaronder begrepen het factureren van MMS-verkeer en debiteurenadministratie alsmede verkeer- en netwerkmanagement, waaronder begrepen transporteren van het verkeer van prepaidklanten naar opwaardeersites en videocompressie, om het gebruik van het netwerk te kunnen analyseren, de continuïteit, beveiliging en integriteit van het netwerk te waarborgen en te bevorderen, (gevolgen van) congestie te beperken en fraude en hoog verbruik te detecteren (onder andere voor bill-shock preventie).”* Vodafone stelt tevens voor om het doeleinde *“Klachtprocessing, afhandeling verzoeken om inlichtingen van klanten/gebruikers en berechting en beslissing van geschillen”* toe te voegen aan de melding. In de concept gewijzigde melding wordt het transporteren van het verkeer van prepaidklanten naar opwaardeersites omschreven. Tevens wordt videocompressie genoemd, onder facturering.

De overige ‘subdoeleinden’ van verkeersbeheer zijn onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving van de concept gewijzigde melding, namelijk: *“om het gebruik van het netwerk te kunnen analyseren.”* Hieruit wordt onvoldoende duidelijk dat Vodafone data-analyse technieken toepast voor netwerkplanning en netwerkmonitoring.

Dit geldt tevens voor het doeleinde ‘beveiliging’. Uit de zinsnede (om) *“de continuïteit, beveiliging en integriteit van het netwerk te waarborgen en te bevorderen”* kan niet worden opgemaakt dat Vodafone data-analysetechnieken toepast op de inhoud van gedownloade bestanden en e-mails voor spam- en virusfiltering en malwarebestrijding.

Naar aanleiding van het onderzoek heeft Vodafone de privacyverklaring van het bedrijf per augustus 2012 aangepast.

Doordat de doeleinden van de gegevensverwerking verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites),

beveiliging (spam- en virusfiltering en malwarebestrijding) en de behandeling van verzoeken om inlichtingen van klanten duidelijk zijn omschreven in de doelomschrijving in het nieuwe Privacy Statement, worden de door Vodafone verzamelde persoonsgegevens voor uitdrukkelijk omschreven doeleinden verzameld en handelt Vodafone ten aanzien van het element 'uitdrukkelijk omschreven' niet langer in strijd met artikel 7 van de Wbp.

Vodafone heeft het CBP, na het sluiten van het onderzoek, medegedeeld dat de [VERTROUWELIJK: apparatuur] sinds vorig jaar niet meer in gebruik is, omdat [VERTROUWELIJK]. Het CBP heeft dit niet nader onderzocht. Voor zover vanaf dat moment van gegevensverwerking geen sprake meer is geweest, zijn de geconstateerde overtredingen ten aanzien van het element 'gerechtvaardigd doeleinde' op dit punt beëindigd.

### 3.9 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.<sup>360</sup>

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:

- op het moment van vastlegging van hem betreffende gegevens, of
- 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,

<sup>360</sup> 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:*

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

hetzij bij derden, hetzij door eigen observatie, bijvoorbeeld naar aanleiding van het gebruik van een netwerk in beheer van de verantwoordelijke.<sup>361</sup>

Deze bepaling vormt een uitwerking van het transparantiebeginsel en het in artikel 6 van de Wbp neergelegde beginsel van 'fair processing'.<sup>362</sup> 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.<sup>363</sup> 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.<sup>364</sup>

Artikel 34 van de Wbp gaat er vanuit dat er geen onderzoeksplicht van de betrokkene is.<sup>365</sup>

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

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

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

Dit alles betekent dat wat betreft het factureringsdoel én voor zover de verwerkingsdoelen verkeersbeheer, opsporing van fraude en behandeling van verzoeken om inlichtingen van abonnees zijn afgeleid van het factureringsdoel, de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst de abonnee of gebruiker in kennis stelt van de soorten (categorieën) verkeersgegevens die worden verwerkt voor deze verwerkingsdoelen, alsmede omtrent de duur van de verwerking. Aanvullend geldt de informatieplicht uit artikel 34 van de Wbp, voor zover het gaat om de verwerking van telecommunicatiegegevens die ook persoonsgegevens zijn.

### Beoordeling

Het CBP heeft in paragrafen 2.4 tot en met 2.7 (p. 22 e.v. van dit rapport) en 3.3 tot en met 3.4 (p. 50 e.v. van dit rapport) vastgesteld dat Vodafone persoonsgegevens die

<sup>361</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 149-150.*

<sup>362</sup> *Idem*, p. 149.

<sup>363</sup> *Idem*.

<sup>364</sup> *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*.

<sup>365</sup> *Idem*, p. 150.

ook verkeersgegevens zijn verwerkt voor de doeleinden verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites), beveiliging (spam- en virusfiltering en malwarebestrijding) en de behandeling van verzoeken om inlichtingen van klanten.

Het CBP heeft in paragraaf 3.5 (p. 63 e.v. van dit rapport) vastgesteld dat Vodafone 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 dataverkeer. Het CBP heeft in paragraaf 2.6 (p. X e.v. van dit rapport) vastgesteld dat Vodafone deze persoonsgegevens die ook communicatie betreffen verwerkt voor het doeleinde beveiliging (in het bijzonder spam- en virusfiltering en malwarebestrijding).

Het CBP heeft in paragrafen 3.3 en 3.4 (p. 50 e.v. van dit rapport) vastgesteld dat de persoonsgegevens over het communicatiegedrag van betrokkenen gegevens van gevoelige aard zijn.

Wat betreft het factureringsdoel én voor zover de verwerkingsdoelen verkeersbeheer, opsporing van fraude en behandeling van verzoeken om inlichtingen van abonnees zijn afgeleid van het factureringsdoel, moet Vodafone betrokkenen in kennis stellen van de soorten (categorieën) verkeersgegevens die worden verwerkt voor deze verwerkingsdoelen, alsmede omtrent de duur van de verwerking. Aanvullend geldt de informatieplicht uit artikel 34 van de Wbp, voor zover het gaat om de verwerking van telecommunicatiegegevens die ook persoonsgegevens zijn, dat Vodafone de betrokkenen onder andere de doeleinden van de verwerking moet mededelen en nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is.

Vodafone informeerde betrokkenen in het oude Privacy Statement en de Algemene Voorwaarden niet volledig en niet duidelijk genoeg over de doeleinden van de verwerking, de categorieën gegevens die werden verwerkt, en over de duur van de verwerking (bewaartermijnen) (zie p. 33 e.v. van dit rapport).

De zinsnede in het oude Privacy Statement van Vodafone 'Ook ten behoeve van het verkeersbeheer voor het netwerk en voor gegevens-uitwisseling met telecombedrijven in het buitenland worden gegevens verwerkt' is te weinig specifiek.

Verder kan Vodafone niet volstaan met de mededeling (in abstracto) in haar Algemene Voorwaarden Consumenten Vodafone Libertel B.V. dat Vodafone persoonsgegevens verwerkt voor 'verkeersbeheer', 'facturatie', 'voorkoming, opsporing en bestrijding van fraude en onregelmatigheden' enz.

De betrokkene zal adequaat moeten worden geïnformeerd (in de woorden van de nieuwe Privacy Statement van Vodafone) dat Vodafone onder andere

- (i) in kaart brengt welke capaciteit de soorten websites en applicaties die door haar klanten worden gebruikt, innemen om eventueel de netwerkcapaciteit kunnen uitbreiden,
- (ii) internetgegevens en informatie verwerkt over hoe het netwerk en de telefoon van een abonnee in combinatie met het netwerk werkt om storingen zo vroeg mogelijk in het netwerk te kunnen signaleren,
- (iii) video's in delen door het netwerk stuurt (zie p. 33 van dit rapport),
- (iv) dat als het prepaid tegoed op is en de klant dit via een mobiele internetpagina wil opladen, naar het dataverkeer kijkt om dit mogelijk te maken,
- (v) netwerkmanagement gebruikt om computervirussen, malware en spam tegen te gaan en
- (vi) bij klantafhandeling over storingen en vragen over de factuur de netwerkgegevens kan gebruiken.

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

Gelet op de gevoelige aard van de persoonsgegevens, de omstandigheden waaronder de persoonsgegevens worden/werden verkregen (te weten: dat onopgemerkt gegevens omtrent betrokkenen worden/werden vergaard en verwerkt, met behulp van automatische procedures voor gegevensvergaring<sup>366</sup> in de vorm van data-analyse technieken) en het gebruik dat ervan wordt/werd gemaakt, is het nodig dat Vodafone de betrokkenen nadere informatie verstrekt(e) over de categorieën van verwerkte gegevens<sup>367</sup> en de bewaartermijn om tegenover de betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen.<sup>368</sup>

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

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

Doordat Vodafone haar abonnees niet volledig en niet duidelijk genoeg informeerde over de hierboven genoemde drie doeleinden van de gegevensverwerking bij de toepassing van data-analyse technieken en ook niet over de categorieën (soorten) van verwerkte gegevens en de duur van de verwerking (bewaartermijnen), handelde Vodafone in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

### **Getroffen maatregelen**

Bij haar zienswijze 1 heeft Vodafone een concept wijziging van haar Privacy Statement toegevoegd. In dit concept wordt een toelichting gegeven op het gebruik van *'internetgegevens en informatie over het hoe het netwerk en jouw telefoon in combinatie met*

<sup>366</sup> Vgl. *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 78.

<sup>367</sup> Vgl. ook artikel 11, eerste lid, onder c, van de Privacyrichtlijn.

<sup>368</sup> Vgl. Last onder dwangsom NS Groep N.V. CBP 9 juni 2011, z2011-00057. URL: [http://www.cbpreweb.nl/downloads\\_pb/pb\\_20110726\\_OV-chip\\_LOD\\_NS.pdf](http://www.cbpreweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_NS.pdf) (URL laatst bezocht op 29 mei 2013).

*het netwerk werkt'. In de voorgestelde wijziging worden de doeleinden verkeersbeheer en facturering, klachtafhandeling, facturering van MMS-berichten en bezoek aan betaalsites door prepaidklanten waarvan het tegoed verbruikt is, toegelicht. Onder verkeersbeheer wordt video-optimalisatie als volgt beschreven: "Zo kunnen we een video bijvoorbeeld in delen door het netwerk sturen." Vodafone schrijft verder: "Ook kijken we naar het totale verkeer van onze klanten, dit doen we anoniem, om bepaalde verkeerstrends te ontdekken (...)."*

Het CBP heeft vastgesteld in paragraaf 2.4 (p. 22 e.v. van dit rapport) dat Vodafone eerst persoonsgegevens verwerkt, alvorens te anonimiseren. Hieruit volgt dat de zinsnede uit de concept wijziging van haar Privacy Statement dat Vodafone anoniem kijkt naar het totale verkeer als feitelijk onjuist moet worden aangemerkt, althans onvolledig en onvoldoende duidelijk is. De betrokkene zal adequaat moeten worden geïnformeerd onder meer over de bewaartermijnen voor de verschillende doeleinden.

Naar aanleiding van het onderzoek heeft Vodafone de privacyverklaring van het bedrijf per augustus 2012 aangepast.

Het CBP heeft in paragraaf 3.8 (p. 91 e.v. van dit rapport) vastgesteld dat de doeleinden van de gegevensverwerking verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites), beveiliging (spam- en virusfiltering en malwarebestrijding) en de behandeling van verzoeken om inlichtingen van klanten duidelijk zijn omschreven in het nieuwe Privacy Statement, evenals de categorieën van verwerkte persoonsgegevens. De overtreding van 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp is in zoverre inmiddels beëindigd.

Dat geldt niet voor de duur van de verwerking (bewaartermijnen).

Doordat de duur van de verwerking/bewaartermijnen onvolledig en onvoldoende duidelijk zijn vermeld in het nieuwe Privacy Statement van Vodafone, duurt de overtreding van artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp op dat punt voort.



### 3.10 Meldingsplicht

#### **Uitwerking van het wettelijk kader**

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

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

#### **Beoordeling**

Het CBP heeft in paragraaf 3.8 (p. 91 e.v. van dit rapport) vastgesteld dat Vodafone de doeleinden - samengevat weergegeven - verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites), beveiliging (spam- en virusfiltering en malwarebestrijding) en de afhandeling van klantklachten waarvoor zij persoonsgegevens verwerkt onvolledig en onvoldoende duidelijk heeft omschreven bij de huidige melding met nummer m1040032 (versienummer 2.0) die Vodafone op 13 maart 2008 heeft gedaan.

Het CBP heeft in paragraaf 2.1 (p. 17 e.v. van dit rapport) vastgesteld dat Vodafone geen andere melding(en) heeft gedaan die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele netwerk. De verwerkingen van persoonsgegevens door Vodafone voor de hierboven genoemde doeleinden voldoen qua doeleinden van de gegevensverwerking en de aard van de verwerkte persoonsgegevens niet aan de eisen die worden gesteld aan de categorieën van vrijgestelde verwerkingen die zijn beschreven in de artikelen van het Vrijstellingsbesluit Wbp. De verwerkingen van persoonsgegevens zijn daarom niet vrijgesteld van de melding (zie paragraaf 3.8, p. X e.v. van dit rapport). Vodafone heeft geen eigen functionaris voor de gegevensbescherming benoemd in de zin van artikel 62 van de Wbp.

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

#### **Voorgenomen maatregelen**

Het CBP heeft in paragraaf 3.8 (p. 91 e.v. van dit rapport) vastgesteld dat Vodafone de doeleinden verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring) en beveiliging (spam- en virusfiltering en malwarebestrijding) waarvoor zij persoonsgegevens verwerkt onvolledig en onvoldoende duidelijk omschrijft in de concept gewijzigde melding. Ook als Vodafone de concept wijzigingen doorvoert, handelt Vodafone nog in strijd met artikel 27 jo. 28 van de Wbp.

#### 4. CONCLUSIES

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

Circa 3,2 miljoen Vodafone abonnees met een (prepaid of postpaid) data abonnement maken gebruik van dataverkeersdiensten van Vodafone.

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

- gegevens over het bezoek aan en gebruik van apps, websites en protocollen voor netwerkplanning
- (technische) gegevens over het functioneren van het netwerk/toestel voor het detecteren en oplossen van problemen in het netwerk (netwerkmonitoring)
- URL's om [VERTROUWELIJK] compressie op video's en webpagina's toe te kunnen passen, tijdens de internet sessie van een abonnee
- URL's om daaraan gratis opwaardeersites te herkennen
- spam-, virus- en malwareherkenningsgegevens uit (gedownload) bestanden en verzonden en ontvangen e-mails
- (technische) gegevens over het functioneren van het netwerk/toestel om verzoeken om inlichtingen van klanten af te handelen

Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn.

De persoonsgegevens worden door Vodafone 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 Vodafone direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon, omdat Vodafone een koppeling(smogelijkheid) heeft met de unieke klant- en/of toestel identifier(s) (bijvoorbeeld het 06-nummer), NAW-gegevens en/of (een) e-mailadres(sen). Er kan dus een relatie tussen de (persoons)gegevens worden gelegd.

De persoonsgegevens zijn in dit rapport ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het 06-nummer), de starttijd en eindtijd van de datasessie, verbruikte datavolume, IP-adres van-naar met poortnummer/protocol, URL's etc.
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer

Vodafone inspecteert en analyseert meestal alleen gegevens over het dataverkeer, niet de inhoud ervan. De gegevens over het dataverkeer kunnen toch inhoudskenmerken bevatten, zoals informatie over bezochte websites en gebruikte apps. Dat soort gegevens die iets (kunnen) zeggen over het gedrag van mensen op internet zijn gevoelige persoonsgegevens waaruit informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie volgt. Alleen gedownload bestanden en verzonden en ontvangen e-mails inspecteert en analyseert

Vodafone ook op inhoud om spam, virussen en malware tegen te houden en te verwijderen.

Vodafone verwerkt de persoonsgegevens voor de volgende onderzochte doeleinden:

- verkeersbeheer en facturering (netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van verkeer van prepaid klanten naar (gratis) opwaardeersites);
- beveiliging (specifiek: spam- en virusfiltering en malwarebestrijding); en
- behandeling van verzoeken om inlichtingen van klanten.

### **Geconstateerde overtredingen**

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

#### Overtredingen die nog niet zijn beëindigd

##### *Meldingsplicht*

Een bedrijf dat persoonsgegevens verwerkt, is in een aantal gevallen op grond van artikel 27 jo. 28 van de Wbp verplicht deze gegevensverwerking te melden bij het CBP. De huidige melding van Vodafone is niet volledig en niet duidelijk genoeg over de doeleinden van de gegevensverwerking verkeersbeheer en facturering (waaronder netwerkplanning, netwerkmonitoring, video-optimalisatie en het transporteren van verkeer van prepaid klanten naar (gratis) opwaardeersites), beveiliging (spam- en virusfiltering en malwarebestrijding) en behandeling van verzoeken om inlichtingen van klanten. Vodafone handelt hierdoor in strijd met artikel 27 jo. 28 van de Wbp.

Vodafone heeft aangegeven bereid te zijn wijzigingen door te voeren in de melding bij het CBP. In het voorstel tot aanpassing van de melding wordt het transporteren van verkeer van prepaidklanten naar opwaardeersites omschreven. Tevens wordt videocompressie genoemd. In het voorstel worden de overige 'subdoeleinden' van verkeersbeheer (netwerkplanning en netwerkmonitoring) niet volledig en niet duidelijk omschreven. Datzelfde geldt voor spam- en virusfiltering en malwarebestrijding.

#### Overtredingen die gedeeltelijk zijn beëindigd

##### *Verkeersbeheer en facturering*

Omdat Vodafone bij aanvang van het onderzoek voor het detecteren en oplossen van problemen in het netwerk de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens bij aanvang van het onderzoek niet zo snel als mogelijk verwijderde, terwijl dat wel mogelijk is en was, had zij gedurende deze verwerkingsduur geen grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Vodafone handelde hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

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

Omdat Vodafone voor netwerkmonitoring via de [VERTROUWELIJK: apparatuur] voor het signaleren van problemen in verband met OS-updates ook zou kunnen volstaan met het bewaren en verwerken van een gedeelte van het [VERTROUWELIJK: identifieer] in plaats van het volledige nummer in de zes maanden geaggregeerde data, heeft zij geen grondslag voor de verwerking van het volledige [VERTROUWELIJK: identifieer] voor het doeleinde verkeersbeheer, gedurende deze verwerkingsduur. Vodafone handelt hierdoor nog in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Doordat Vodafone voor het detecteren en oplossen van problemen in het netwerk de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens voor het overige inmiddels wel zo snel als mogelijk verwijderd, heeft zij in dat verband een grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Op die punten is Vodafone niet langer in overtreding (grondslag).

#### Overtredingen die zijn beëindigd

##### *Verkeersbeheer en facturering*

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

Omdat Vodafone voor netwerkplanning de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens niet zo snel als mogelijk verwijderde, terwijl dat wel mogelijk is en was, had zij, na het verzamelen daarvan, geen grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer. Vodafone handelde hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Vodafone heeft het CBP, na het sluiten van het onderzoek, medegedeeld dat de [VERTROUWELIJK: apparatuur] sinds vorig jaar niet meer in gebruik is, omdat [VERTROUWELIJK]. Het CBP heeft dit niet nader onderzocht. Voor zover vanaf dat moment van gegevensverwerking geen sprake meer is geweest, zijn de geconstateerde overtredingen op dit punt beëindigd.

Om prepaid abonnees in staat te stellen opwaardeersites te bezoeken als hun tegoed op is, verwerkte Vodafone bij aanvang van het onderzoek URL's om de gratis opwaardeersites te herkennen. Omdat er ook andere mogelijkheden zijn en waren, was deze gegevensverwerking onevenredig. Vodafone handelde hierdoor in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp.

Vodafone verleent thans toegang tot gratis opwaardeersites op basis van [VERTROUWELIJK]. Dit is in deze context een proportionele implementatie van het bieden van opwaardeermogelijkheden bij een ontoereikend prepaid tegoed, direct via 'mobiel internet', gelet op de omstandigheid dat de verwerkte gegevens niet worden

opgeslagen en bewaard. Door deze aanpassing handelt Vodafone op dit punt niet langer in strijd met artikel 11.5 van de Tw jo. artikel 8 van de Wbp (grondslag).

#### *Informeren abonnees*

Vodafone 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. Vodafone informeerde abonnees bij aanvang van het onderzoek niet volledig en niet duidelijk genoeg over de hierboven genoemde drie doeleinden van de gegevensverwerking bij de toepassing van data-analyse technieken. Daarnaast informeerde Vodafone hen niet over de categorieën (soorten) van verwerkte gegevens en de duur van de verwerking (bewaartermijnen). Vodafone handelde hierdoor in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

Vodafone heeft de privacyverklaring van het bedrijf per augustus 2012 aangepast.

Vodafone informeert abonnees in haar nieuwe Privacy Statement niet volledig en niet duidelijk over de bewaartermijnen. Vodafone handelt hierdoor nog in strijd met artikel 11.5, vierde lid, van de Tw jo. artikel 34 van de Wbp.

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

#### *Uitdrukkelijk omschreven en gerechtvaardigde doeleinden*

Doordat Vodafone de hiervoor genoemde drie doeleinden waarvoor zij persoonsgegevens verwerkt onvolledig en onvoldoende duidelijk heeft omschreven bij de melding die zij heeft gedaan en Vodafone abonnees bij aanvang van het onderzoek ook niet in haar oude Privacy Statement over deze doeleinden informeerde, werden de door Vodafone verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld.

Doordat de gegevensverwerking voor de doeleinden verkeersbeheer en facturering (specifiek: netwerkplanning, netwerkmonitoring en het transporteren van verkeer van prepaid klanten naar (gratis) opwaardeersites) bij aanvang van het onderzoek niet in alle stadia kon steunen op een of meer van de in artikel 11.5 van de Tw jo. artikel 8 van de Wbp genoemde gronden, werden de door Vodafone verzamelde persoonsgegevens niet voor gerechtvaardigde doeleinden verzameld.

Vodafone handelde hierdoor in strijd met 7 van de Wbp.

Doordat Vodafone in haar nieuwe Privacy Statement wel informeert over de drie doeleinden waarvoor zij persoonsgegevens verwerkt, handelt Vodafone op dit punt niet langer in strijd met artikel 7 van de Wbp (uitdrukkelijk omschreven doeleinden).

Voor zover de [VERTROUWELIJK: apparatuur] sinds vorig jaar niet meer in gebruik is, handelt Vodafone op dit punt niet langer in strijd met artikel 7 van de Wbp (gerechtvaardigde doeleinden).

De overtreding die inhoudt het verzamelen van persoonsgegevens zonder gerechtvaardigd doeleinde vanwege het verwerken zonder grondslag duurt wel voort voor de gegevensverwerking voor netwerkmonitoring via de [VERTROUWELIJK: apparatuur], wat betreft één bewaartermijn van persoonsgegevens (het volledige [VERTROUWELIJK: identifier] in de zes maanden geaggregeerde data).

Doordat Vodafone de via de [VERTROUWELIJK: apparatuur] verzamelde persoonsgegevens voor netwerkmonitoring voor het overige inmiddels wel zo snel als mogelijk verwijdert en doordat zij thans toegang tot gratis opwaardeersites verleend op basis van [VERTROUWELIJK], heeft zij in dat verband een grondslag voor de gegevensverwerking voor het doeleinde verkeersbeheer en facturering. Hierdoor handelt Vodafone op deze punten niet langer in strijd met artikel 7 van de Wbp (gerechtvaardigde doeleinden).

#### Geen overtredingen geconstateerd

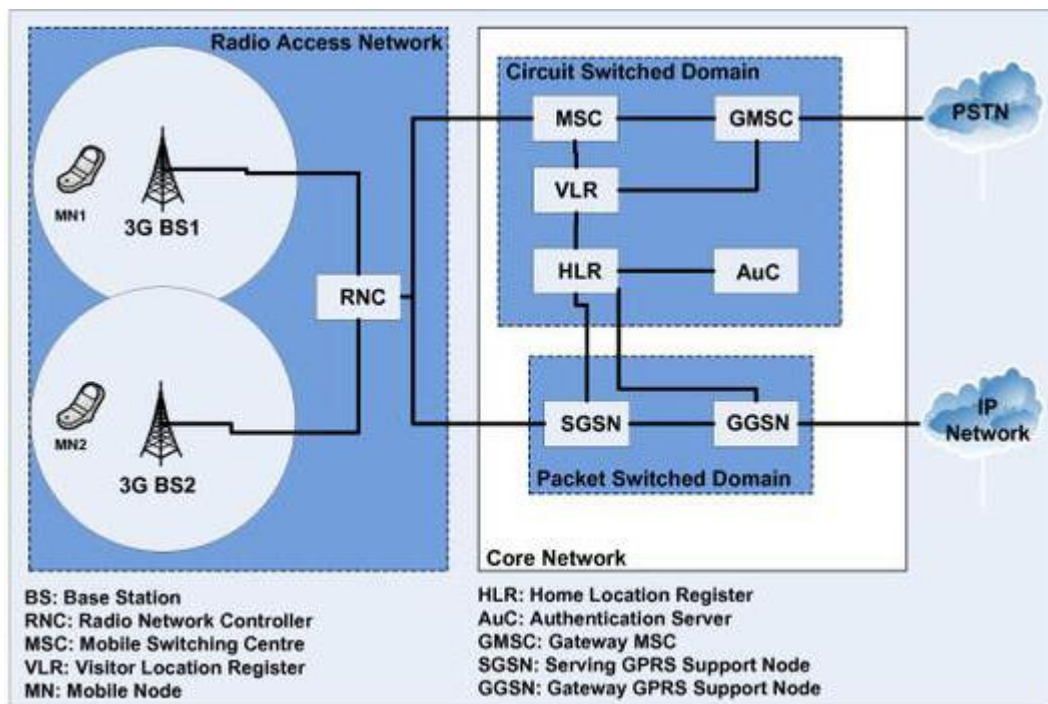
##### *Verkeersbeheer en facturering*

Omdat Vodafone voor netwerkplanning via de [VERTROUWELIJK: apparatuur] de persoonsgegevens zo snel als mogelijk onomkeerbaar anonimiseert, heeft zij in zoverre een wettelijke grondslag voor deze verwerking ten behoeve van verkeersbeheer. Op dit punt is Vodafone dan ook niet in overtreding (geweest).

Naar aanleiding van het onderzoek heeft Vodafone bovendien de bewaartermijnen van de geanonimiseerde gegevens voor netwerkplanning via de [VERTROUWELIJK: apparatuur] verkort.

##### *Video-optimalisatie, spam- en virusfiltering & malwarebestrijding en klachtbehandeling*

Vodafone heeft wel een wettelijke grondslag voor de verwerking ten behoeve van video-optimalisatie, spam- en virusfiltering en malwarebestrijding en behandeling van verzoeken om inlichtingen van klanten. Op deze punten is Vodafone dan ook niet in overtreding (geweest).



<sup>369</sup> Illustratie uit Fragkiadakis et al.: **Ubiquitous robust communications for emergency response using multi-operator heterogeneous networks**. *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:13, gebruikt onder Creative Commons Attribution licentie, <http://creativecommons.org/licenses/by/2.0/>. URL: <http://jwcn.eurasipjournals.com/content/pdf/1687-1499-2011-13.pdf> (URL laatst bezocht op 29 mei 2013).

## Bijlage II Overzicht verwerkte gegevens, per doeleinde

### Netwerkplanning en het transporteren van verkeer van prepaid klanten naar (gratis) opwaardeersites\* ([VERTROUWELIJK: apparatuur])

|                                                            |
|------------------------------------------------------------|
| VERTROUWELIJK (identifiers)                                |
| hostname (URL op hoofddomein) van de website/app           |
| IP-adres van-naar met poortnummer/protocol [VERTROUWELIJK] |
| verbruikte datavolume [VERTROUWELIJK]                      |
| start- en eindtijd sessie/tijdsvenster                     |
| URL*                                                       |

### Netwerkplanning ([VERTROUWELIJK: apparatuur])

|                                                  |
|--------------------------------------------------|
| [VERTROUWELIJK: identifiers]                     |
| VERTROUWELIJK                                    |
| URL van de website/app                           |
| hostname (URL op hoofddomein) van de website/app |
| IP-adres van-naar met poortnummer/protocol       |
| verbruikte datavolume                            |
| start- en eindtijd sessie/tijdsvenster           |

### Netwerkmonitoring en behandeling van verzoeken om inlichtingen van klanten ([VERTROUWELIJK: apparatuur])

|                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------|
| [VERTROUWELIJK: identifiers]                                                                                                                |
| [VERTROUWELIJK] <ul style="list-style-type: none"><li>• hostname (URL op hoofddomein)</li><li>• IP-adres van-naar met poortnummer</li></ul> |
| start- en eindtijd sessie/tijdsvenster                                                                                                      |
| verbruikte datavolume [VERTROUWELIJK]                                                                                                       |

### Beveiliging ([VERTROUWELIJK: apparatuur])

|                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| unieke klant- en/of toestelidentificer(s)                                                                                                                                                                                                                                                    |
| [VERTROUWELIJK]                                                                                                                                                                                                                                                                              |
| inhoud van door abonnees gedownloade bestanden en verzonden en ontvangen e-mails aan de hand van vooraf gedefinieerde spam-, virus- en malwareherkenningspatronen, voor zover nodig om spam/virussen/malware tegen te houden en te verwijderen (spam-, virus- en malwareherkenningsgegevens) |

### Behandeling van verzoeken om inlichtingen van klanten ([VERTROUWELIJK: apparatuur])

|                                 |
|---------------------------------|
| [VERTROUWELIJK]                 |
| URL van het gedownloade bestand |
| [VERTROUWELIJK]                 |



### Bijlage III Verklarende woordenlijst

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

|                                                                                |                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Identity)</i>                                                               | wereldwijd uniek 15-cijferig nummer, opgeslagen op de SIM-kaart van de mobiele telefoon. De eerste drie nummers zijn de landcode (in Nederland bijvoorbeeld 204), gevolgd (in Europa) door twee nummers die de aanbieder van het netwerk in dat land identificeren waar de klant abonnee is. |
| 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 afwikkelen van telefonie- en dataverkeer via het netwerk van zendmasten.                                                                                                                                                      |
| Radioweg                                                                       | De radioweg ofwel <i>air-interface</i> is het deel van de communicatieketen dat toegang biedt tot het radiotoegangsnetwerk.                                                                                                                                                                  |
| Roaming                                                                        | Techniek om telefonie- 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 afwikkelen 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 IV Zienswijze 1 Vodafone, met de reactie daarop van het CBP (zoals weergegeven in het Conceptrapport definitieve bevindingen, gegroepeerd én aangevuld met in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van dat Conceptrapport definitieve bevindingen).

#### Opmerkingen en aanvullingen feitelijk kader

##### *OSI-model*

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat het CBP de bevinding dat Vodafone zowel verkeersgegevens als inhoud van de communicatie verwerkt, baseert op een onjuiste weergave en analyse van het OSI-model. Het CBP gebruikt een foutieve versie van het model, omdat het miskent dat elk datapakket op elke protocollaag van het OSI-model een header heeft. Vodafone schrijft dat zij uitsluitend kennis neemt, op elke laag van het model, van de header. *“In deze ‘header’ bevinden zich onder meer adresgegevens, zoals de URL (...).”*<sup>370</sup> In haar zienswijze benadrukt Vodafone dat er *“geen harde onderverdeling [is, toevoeging door het CBP] te maken tussen gegevens uit en over het dataverkeer: doorslaggevend is dat Vodafone van de inhoud vandaan blijft en enkel de header inspecteert.”*<sup>371</sup> Vodafone geeft aan dat het gebruikte protocol (zoals de Skype dienst) er toe kan leiden dat de adresgegevens niet in een header zitten op een niveau lager dan de OSI-laag 7.<sup>372</sup>

**Reactie CBP:** Het OSI-model wordt hier niet gebruikt als een normatief model dat voorschrijft op welke wijze een telecommunicatienetwerk moet zijn ingericht, maar als hulpmiddel om processen en gegevensstromen in een netwerk te kunnen aanduiden. De omstandigheid dat zo’n model altijd een vereenvoudiging is van de werkelijkheid, doet niet af aan de waarde daarvan als hulpmiddel. Ter verduidelijking is tevens de (door Vodafone voorgestelde) vergelijking met het TCP-IP model opgenomen in dit rapport. Het kan overigens nog eenvoudiger. Het Europese samenwerkingsverband van telecomtoezichthouders, BEREC, deelt in de recente concept netneutraliteitsrichtsnoeren het netwerkverkeer in twee lagen in, te weten: een netwerklaag en een applicatie/contentlaag. BEREC schrijft: *“When running an application, the end user is making use of the electronic communication service at the network layer. The application software installed on the terminal equipment (also referred to as the host) executes functions at the application/content layer (...). Applications (e.g. telephony, television and web) and content (e.g. videos and web pages) are produced in the endpoints which communicate with each other using the underlying network layer. In these guidelines, the content/application layer is referred to simply as the application layer, while recognising that it actually contains both content and applications.”*<sup>373</sup>

---

<sup>370</sup> Zienswijze 1 Vodafone, randnummer 7.

<sup>371</sup> Idem, randnummer 36.

<sup>372</sup> Idem, randnummers 7 en 22.

<sup>373</sup> BEREC Guidelines for Quality of Service in the scope of Net Neutrality, Draft for public consultation, 29 May 2012, p. 15-16, URL: [http://berec.europa.eu/doc/consult/bor\\_12\\_32\\_guidelines.pdf](http://berec.europa.eu/doc/consult/bor_12_32_guidelines.pdf).

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

Ten aanzien van een VoIP-dienst zoals Skype geldt echter, zoals Vodafone in haar zienswijze 1 ook aangeeft, dat de ontwikkelaars technische maatregelen hebben getroffen om herkenning van het verkeer te bemoeilijken, zoals het gebruik van 'betekenisloze headers', het dynamisch toewijzen van poorten en het versleutelen van de inhoud van de berichten. Herkenning/identificatie van Skype-verkeer geschiedt daarom in de praktijk veelal door middel van uitgebreidere *signature based identification*. Dat wil zeggen, aan de hand van vooraf gedefinieerde patronen gebaseerd op de unieke eigenschappen van het protocol ('fingerprints'), zoals de lengte en de frequentie van verzonden en ontvangen packets bij de start van een Skype-sessie (bijvoorbeeld de eerste tien) in combinatie met (de eerste packets van de) inhoud van het verkeer/payload.<sup>374</sup>

Vodafone noemt dit zelf *deep packet inspection* in haar reactie op het inlichtingenverzoek van OPTA: *"Bij gebruik van een applicatie zoals VoIP kunnen we niet aan de header zien welk protocol wordt gebruikt, we kijken dan naar een 'fingerprint'. Deze fingerprint zit in het begin van de datasessie, er vindt namelijk een signaleringsmoment plaats, de eerste paar bytes die in een verkeersstroom worden uitgewisseld zijn nodig om vast te stellen of VoIP gebruik door de aanvrager mogelijk is. VoIP moet - net als bij een gewoon mobiel telefoongesprek - eerst een verbinding opbouwen. Er wordt door Vodafone alleen op dat 'signaleringsmoment' een datasessie geïnspecteerd. We passen dan dus inderdaad deep packet inspection toe, maar er wordt nooit naar de uitgewisselde inhoud - het gesprek of de e-mail- gekeken."*<sup>375</sup>

<sup>374</sup> [VERTROUWELIJK] Zie verder bijvoorbeeld Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, Paolo Tofanelli, Revealing skype traffic: when randomness plays with you, ACM SIGCOMM Conference - SIGCOMM, p. 37-48, 2007. URL: <http://dl.acm.org/citation.cfm?id=1282386> "Following a closed source and proprietary design, Skype protocols and algorithms are unknown. Moreover, strong encryption mechanisms are adopted by Skype, making it very difficult to even glimpse its presence from a traffic aggregate." Vgl. Dario Rossi, Marco Mellia, Michela Meo, Following Skype Signaling Footsteps, Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. URL: <http://www.tlc-networks.polito.it/oldsite/mellia/papers/skype-qosip.pdf>: "From a protocol perspective, Skype uses a proprietary solution which is difficult to reverse engineer due to extensive use of both cryptography and obfuscation techniques. Though Skype may rely on either TCP or UDP at the transport layer, both signaling and communication data are preferentially carried over UDP. A single random port is selected during application installation, and it is never changed (unless forced by the user). When a UDP communication is impossible, Skype falls back to TCP, listening to the same random port, and port 80 and 443 which are normally left open by network administrators to allow Web browsing." Vgl. P. Svoboda, E. Hyytia, F. Ricciato, M. Rupp, M. Karner, Detection and Tracking of Skype in a live 3G Network exploiting Cross Layer Information, 1st Int'l Workshop on Traffic Monitoring and Analysis (TMA 2009) 11 May 2009, Aachen, Germany. Published in LNCS vol. 5537. URL: [http://publik.tuwien.ac.at/files/PubDat\\_184256.pdf](http://publik.tuwien.ac.at/files/PubDat_184256.pdf). Vergelijk ook de recente guidance van het Nieuw-Zeelandse cyber security centre over Skype. NCSC, Guidance Regarding Skype and Other P2P VoIP Solutions, Ver. 1.1 June 2012, URL: <http://ncsc.govt.nz/sites/default/files/articles/NCSC-Skype%20Guidance%201.1.pdf>: "Some P2P applications, such as Skype, use proprietary protocols and make use of encrypted tunnels to bypass firewalls. As a result, their use is extremely difficult to regulate or monitor."

<sup>375</sup> Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

Vodafone bevestigt dit in haar zienswijze 1: "[VERTROUWELIJK]."<sup>376</sup>

[VERTROUWELIJK]

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

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

*Noodzaak verkeersbeheer*

**Zienswijze 1 Vodafone:** In haar zienswijze 1 schrijft Vodafone dat verkeersbeheer (ook) noodzakelijk is om het netwerk goed te laten *blijven* functioneren, ondanks de explosieve toename van het datagebruik als gevolg van smartphones en tablets: *"Dataverkeer over mobiele netwerken nam de afgelopen 4 jaar met een factor 2-3 per jaar toe. Het totale mobiele dataverkeer in 2011 was een factor 8 van het mondiale dataverkeer (vast en mobiel) in 2000. (...) Smartphones vertegenwoordigen 82% van het dataverkeer. (...) In de komende vier jaar zal het mobiele dataverkeer met een factor 18 groeien. (...) Netwerkbeheer en -forecasting betekent, gelet op deze cijfers, kortom dat dagelijks alle zeilen moeten worden bijgezet om het netwerk te laten blijven functioneren (...)."*<sup>377</sup>

In haar zienswijze 1 vult Vodafone aan dat het noodzakelijk voor haar is om op individueel klantniveau gegevens te verwerken om valide, bruikbare informatie te krijgen over de netwerkbelasting als gevolg van de toename van het gebruik van allerlei websites en apps (ten behoeve van netwerkplanning en -beheer).<sup>378</sup> "[VERTROUWELIJK]"<sup>379</sup> Aanvullend licht Vodafone toe: *"Vodafone moet de oorzaak van de druk op het signaleringskanaal in kaart brengen om deze druk vervolgens te kunnen managen. Ter voorkoming van misverstanden: hierbij gaat het niet om 'de populariteit' of iets dergelijks van de verschillende toestellen en/of apps te controleren, maar de mate van netwerkbelasting. Zo weet Vodafone, door gebruik te maken van de door het CBP onderzochte technieken, dat er zelfs tussen verschillende merken smartphones grote verschillen kunnen bestaan wat de druk op het signaleringskanaal betreft. [VERTROUWELIJK]."*<sup>380</sup>

In haar zienswijze 1 vult Vodafone (daarnaast) aan dat Vodafone zich voor monitoring ook baseert "[VERTROUWELIJK]."<sup>381</sup>

Vodafone schrijft (ten slotte) dat zij ook dit soort initiatieven ontplooit met fabrikanten van toestellen (te weten: om de gebruikte software anders in te richten, op een manier

---

<sup>376</sup> Zienswijze 1 Vodafone, randnummer 98.

<sup>377</sup> Idem, randnummers 26-28.

<sup>378</sup> Idem, randnummer 107.

<sup>379</sup> Idem, randnummer 90.

<sup>380</sup> Idem, randnummer 32.

<sup>381</sup> Idem, randnummer 29.

die netwerkvriendelijker is) maar dat deze initiatieven uiteraard niet meteen hun vruchten afwerpen.<sup>382</sup>

**Reactie CBP:** De zienswijze 1 van Vodafone heeft op het punt van de noodzaak van data-analyse geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

[VERTROUWELIJK: apparatuur]

**Zienswijze 1 Vodafone:** Vodafone geeft in haar zienswijze 1 een technische toelichting op (de werkwijze van Vodafone bij) de inzet van de [VERTROUWELIJK: apparatuur]: *"Dit [[VERTROUWELIJK], toevoeging door het CBP] gaat weliswaar om gedetailleerde informatie doch deze is uitsluitend afkomstig uit de headers. Ter illustratie: voorzover het om de URL gaat, betreft het alleen de homepage dus zonder gegevens over subpagina's van de bezochte site. Ook de inhoud van de site is geen onderdeel van de ruwe data."*<sup>383</sup> Ten aanzien van de locatiegegevens verklaart Vodafone dat zendmastgegevens niet in het netwerk beschikbaar zijn en dus door geen enkele applicatie worden verwerkt.<sup>384</sup>

In haar zienswijze 1 schrijft Vodafone (verder) dat slechts twee streng geselecteerde werknemers van Vodafone kunnen controleren, onder strikte voorwaarden, wat er in het netwerk op datapakket niveau gebeurt, terwijl er maar vier werknemers toegang hebben tot de geaggregeerde rapporten.<sup>385</sup>

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

**Zienswijze 1 Vodafone:** In haar zienswijze 1 geeft Vodafone aan dat in de [VERTROUWELIJK] apparatuur "[VERTROUWELIJK]."<sup>386</sup>

**Reactie CBP:** Tijdens het onderzoek ter plaatse heeft het CBP inzage gehad in de gebruikersinterface van de apparatuur. Hieruit blijkt dat de statistiek van grootste dataverbruikers op [VERTROUWELIJK: identifier], en dus op klantniveau wordt geaggregeerd. De [VERTROUWELIJK: identifiers] zijn daarbij zichtbaar in de gebruikersinterface.

De zienswijze 1 van Vodafone heeft op het punt van (de werkwijze van Vodafone bij) de inzet van data-analyse technieken geleid tot verduidelijking van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve.

---

<sup>382</sup> Idem, randnummer 32, voetnoot 11.

<sup>383</sup> Idem, randnummer 39.

<sup>384</sup> Idem, randnummer 88.

<sup>385</sup> Idem, randnummer 37.

<sup>386</sup> Idem, randnummer 40.

**Zienswijze 1 Vodafone:** In haar zienswijze verklaart Vodafone dat zij *"een streng toezichts- en controlesysteem [heeft, toevoeging door het CBP] waardoor dit [te weten: rapportages uitdraaien op individueel klantniveau met de gegevens, toevoeging door het CBP] de facto niet kan plaatsvinden en ook niet plaatsvindt.*<sup>387</sup>

**Reactie CBP:** [VERTROUWELIJK]

De zienswijze 1 van Vodafone heeft op het punt van (de werkwijze van Vodafone bij) de inzet van data-analyse technieken geleid tot verduidelijking van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

[VERTROUWELIJK: apparatuur]

**Zienswijze 1 Vodafone:** Vodafone geeft in haar zienswijze 1 een technische toelichting op (de werkwijze van Vodafone bij) de inzet van de [VERTROUWELIJK: apparatuur]. In haar zienswijze 1 licht Vodafone toe dat de gegevens na een uur worden geaggregeerd, "[VERTROUWELIJK]."<sup>388</sup> Vodafone verklaart verder dat de gegevens na een uur per groep van abonnees/website, app of protocol worden geaggregeerd, [VERTROUWELIJK] worden opgeslagen en gedurende 15 dagen tot 24 maanden worden bewaard.<sup>389</sup> [VERTROUWELIJK]

Vodafone geeft aan dat zij haar leverancier heeft gevraagd de bewaartermijnen verder te verkorten. De bewaartermijn (van de geaggregeerde gegevens) is voortaan:

*"uuraggregatie: 14 dagen*

*-dagaggregatie: 32 dagen*

*-maandaggregatie: 13 maanden"*<sup>390</sup>

Vodafone licht (verder) toe in haar zienswijze: *"In [VERTROUWELIJK: apparatuur] is geaggregeerde data beschikbaar die aangeeft hoe vaak een klantgroep (bijvoorbeeld de prepaidklanten; kortom verre van individueel) een bepaalde website (www.nu.nl) bezoekt, maar niet het werkelijke surfgedrag."*<sup>391</sup>

**Reactie CBP:** De zienswijze 1 van Vodafone heeft op het punt van (de werkwijze van Vodafone bij) de inzet van data-analyse technieken geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen).

[VERTROUWELIJK: apparatuur]

**Zienswijze 1 Vodafone:** Vodafone geeft in haar zienswijze 1 een technische toelichting op (de werkwijze van Vodafone bij) de inzet van de [VERTROUWELIJK: apparatuur]. Vodafone schrijft dat de [VERTROUWELIJK: apparatuur] géén

---

<sup>387</sup> Idem, randnummer 41.

<sup>388</sup> Idem, randnummer 50.

<sup>389</sup> [VERTROUWELIJK]

<sup>390</sup> Zienswijze 1 Vodafone, randnummer 52.

<sup>391</sup> Idem, randnummer 53.



zendmastgegevens verwerkt: *"Zoals opgemerkt in onze zienswijze worden bij Vodafone geen zendmastgegevens van klanten met toegang tot mobiel netwerk vanuit het netwerk geleverd. [VERTROUWELIJK]."*<sup>392</sup>

**Reactie CBP:** [VERTROUWELIJK]

De zienswijze 1 van Vodafone heeft op het punt van (de werkwijze van Vodafone bij) de inzet van data-analyse technieken geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft wel geleid tot gedeeltelijke aanpassing van de conclusies in het Rapport definitieve bevindingen).

**Zienswijze 1 Vodafone:** In haar zienswijze 1 licht Vodafone toe dat de bewaartermijn van 7 dagen [inmiddels 2 dagen, toevoeging door het CBP] noodzakelijk is om het systeem terug te kunnen zetten na een eventuele crash: *"[VERTROUWELIJK]."*<sup>393</sup>

Aanvullend licht Vodafone toe dat [VERTROUWELIJK]

Tevens schrijft Vodafone: *"[VERTROUWELIJK]."*<sup>394</sup>

**Reactie CBP:** Het CBP begrijpt deze informatie als volgt. [VERTROUWELIJK]

De zienswijze 1 van Vodafone heeft op het punt van (de werkwijze van Vodafone bij) de inzet van data-analyse technieken geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft wel geleid tot gedeeltelijke aanpassing van de conclusies in het Rapport definitieve bevindingen).

*(Algemene) technische en organisatorische maatregelen*

**Zienswijze 1 Vodafone:** Vodafone voegt in haar zienswijze 1 toe dat zowel op de [VERTROUWELIJK: apparatuur] als op de [VERTROUWELIJK: apparatuur] apparatuur *"autorisatie, authenticatie en account beheer processen en procedures van toepassing [zijn, toevoeging door het CBP] waarvan de correcte naleving zorgvuldig wordt gecontroleerd. Voor zover deze processen en procedures onderdeel zijn van SOX regelgeving worden zij ook periodiek door een externe auditor gecontroleerd."*<sup>395</sup>

**Reactie CBP:** De zienswijze 1 van Vodafone heeft op het punt van (algemene) technische en organisatorische maatregelen geleid tot verduidelijking en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

---

<sup>392</sup> E-mail Vodafone van 10 juli 2012.

<sup>393</sup> Idem, randnummer 58.

<sup>394</sup> Zienswijze 1 Vodafone, randnummer 60.

<sup>395</sup> Idem, randnummer 37. Als Bijlage 1 bij de Zienswijze is een kopie gevoegd van de [VERTROUWELIJK].

## Verwerking van persoonsgegevens

### *Postpaid abonnees*

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat het CBP voorbij gaat *"aan het feit dat de meeste gegevens niet toegankelijk zijn voor Vodafone medewerkers, of anderen, en slechts worden gebruikt in het kader van doorvoer. Vodafone hanteert daartoe bovendien een strikt beveiligingsbeleid en controleert dat geen toegang is verkregen, of kan zijn, tot bepaalde gegevens. Vodafone's medewerkers worden daarnaast getraind op privacy- en beveiligingsaspecten. (...) Ook zijn veel gegevens slechts in geanonimiseerde of geaggregeerde vorm beschikbaar en dus om die reden geen persoonsgegevens."*<sup>396</sup>

**Reactie CBP:** Ten aanzien van de door Vodafone gehanteerde technische en organisatorische maatregelen, waaronder toegangsautorisaties (slechts een selecte groep medewerkers heeft toegang tot gebruik van de data analyse apparatuur), toegangsbeveiliging en controle daarop geldt dat dit bovenal een technische en organisatorische waarborg betreft ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens zoals bedoeld in artikel 13 van de Wbp.<sup>397</sup> De omstandigheid dat slechts bepaalde medewerkers toegang hebben tot de data-analyse apparatuur en de data die met behulp daarvan wordt verwerkt, leidt echter niet tot de conclusie dat er geen sprake is van persoonsgegevens. De toegepaste aggregatie op abonnee-niveau (via de [VERTROUWELIJK: apparatuur] en de [VERTROUWELIJK: apparatuur]) is geen anonimisering<sup>398</sup> of gegevensvernietiging.

Dit geldt ook voor de versleutelde [VERTROUWELIJK: identifiers] in de [VERTROUWELIJK] voor verkeersbeheer doeleinden. [VERTROUWELIJK]

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

### *Prepaid abonnees*

**Zienswijze 1 Vodafone:** In haar zienswijze 1 stelt Vodafone dat er bij prepaid abonneementen geen sprake is van persoonsgegevens *"omdat er dan geen identificerende gegevens betreffende de abonnee beschikbaar zijn."*<sup>399</sup>

**Reactie CBP:** Ten aanzien van de prepaid abonnees van wie Vodafone geen NAW-gegevens en/of e-mailadressen heeft, beschikt Vodafone wel over ten minste MSISDN (een direct contactgegeven), IMSI- en/of IMEI-nummer en IP-adres.<sup>400</sup> Vodafone heeft,

---

<sup>396</sup> Idem, randnummer 87.

<sup>397</sup> Naleving van het bepaalde in artikel 13 van de Wbp (beveiliging) valt buiten de scope van dit onderzoek.

<sup>398</sup> Anonimiseren wordt in de wetsgeschiedenis bij de Wbp gedefinieerd als *"een vorm van vernietigen van persoonsgegevens althans in de gevallen dat de verwijdering van de naam ook tot gevolg heeft dat de betrokkene niet meer kan worden herleid. Alleen in dit laatste geval pleegt te worden gesproken van «anonimiseren»."* Kamerstukken II 1999/2000, 25 892, nr. 92c, p. 13.

<sup>399</sup> Zienswijze 1 Vodafone, p. 27.

<sup>400</sup> Zie HvJ EU 24 november 2011, zaak C-70/10 (Scarlet/Sabam), r.o. 26 over de status van OPENBARE VERSIE Rapport definitieve bevindingen 29 mei 2013

zoals hiervoor in dit Conceptrapport definitieve bevindingen 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).<sup>401</sup>

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.”*<sup>402</sup>

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

#### Samenloop Wbp en Tw: grondslagtoetsing

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat alle gegevens verkeersgegevens zijn en dat daarom van een grondslag onder de Wbp geen sprake kan zijn. Vodafone schrijft: *“Dit betekent dat in het samenstel van de Tw en de Wbp primair de vraag moeten worden beantwoord of Vodafone aan de verwerkings- en anonimiseringsvereisten van de Tw -artikel 11.5 Tw- voldoet. Is dat het geval, dan kan er geen sprake van zijn dat er geen grondslag zou bestaan voor die(zelfde) verwerking onder de Wbp.”*<sup>403</sup>

Aanvullend schrijft Vodafone: *“Dat alle verwerkte gegevens verkeersgegevens zijn staat voor Vodafone vast. (…)* Ook bij (mobiele) telefonie moet elke aanbieder al sinds

---

IP-adressen, die persoonsgegevens vormen.

<sup>401</sup> WP29 136. Advies 4/2007 over het begrip persoonsgegevens, 20 juni 2007, p. 14-15.

<sup>402</sup> HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

<sup>403</sup> Zienswijze 1 Vodafone, randnummer 83.

*jaar en dag de verschillen tussen - bijvoorbeeld 0800-nummers, 0900-nummers, lokaal tarief, interlokaal tarief etc. kunnen (door)berekenen aan respectievelijk voor haar klanten. Vodafone moet daarvoor de zogenaamde B-nummers (lees: de bestemming van het gesprek/verkeer) dus kunnen herkennen om correct te kunnen factureren. Het door het CBP geschetste heeft dus geen (speciale) relevantie voor dataverkeer.”<sup>404</sup>*

**Reactie CBP:** Het CBP heeft in dit Conceptrapport definitieve bevindingen vastgesteld dat de persoonsgegevens kunnen worden ingedeeld in twee categorieën:

1. persoonsgegevens die tevens communicatie zijn (en dus geen verkeersgegevens), namelijk gegevens zoals hostnames (URL op hoofddomein), volledige URL's en app/ protocol/service en virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer
2. persoonsgegevens die tevens verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het telefoonnummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume etc.

Elke categorie van persoonsgegevens heeft een eigen beoordelingskader.

**Persoonsgegevens, tevens communicatie: hostnames, URL's en app/ protocol/service en spam-, virus- en malwareherkenningsgegevens**

Ten aanzien van hostnames, URL's en app/ protocol/service en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer, geldt dat geen sprake is van verkeersgegevens, maar van communicatie (tevens persoonsgegevens).<sup>405</sup> Artikel 8 van de Wbp is van toepassing, zij het dat (richtlijnconforme uitleg<sup>406</sup> 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.

Mogelijke grondslagen

*Verkeersbeheer: facturering/uitvoering van een overeenkomst/gerechtvaardigd belang*

**Zienswijze 1 Vodafone:** Subsidiair vult Vodafone aan dat als aan artikel 11.5 Tw wordt voldaan, er een grondslag bestaat ex artikel 8, sub b, (overeenkomst met de abonnees), subsidiair 8, sub f, van de Wbp.<sup>407</sup>

---

<sup>404</sup> Idem, randnummer 91.

<sup>405</sup> 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.

<sup>406</sup> 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*).

<sup>407</sup> Zienswijze 1 Vodafone, randnummer 103 e.v.

Vodafone schrijft in haar zienswijze 1 dat gegevens die worden verwerkt zoals het gebruik door betrokkenen van bepaalde websites, apps, VOIP etc *"worden verwerkt omdat dit noodzakelijk is om facturering - en dus: uitvoering van de overeenkomst - mogelijk te maken."*<sup>408</sup>

**Reactie CBP:** Het CBP heeft in dit Conceptrapport definitieve bevindingen vastgesteld dat de gegevens die Vodafone verwerkt niet alleen verkeersgegevens, tevens persoonsgegevens zijn, maar ten dele ook communicatie (tevens persoonsgegevens).

De door Vodafone genoemde grondslagen worden door het CBP hieronder besproken, en in het vervolg van deze zienswijzenbespreking onder het kopje 'Technische alternatieven'.

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

De persoonsgegevens zijn niet noodzakelijk voor de uitvoering van het mobiele telefoniecontract, meer in het bijzonder het (prepaid of postpaid) data abonnement, met de betrokkene omdat Vodafone geacht moet worden ook zonder de gegevens van *deze specifieke individuele betrokkene* de overeengekomen telecommunicatiedienst(en) (in casu: mobiele datadiensten) te kunnen leveren. Het CBP heeft in dit Conceptrapport definitieve bevindingen vastgesteld dat Vodafone via de data-analyse apparatuur gegevens over en uit het dataverkeer van alle ongeveer 3,2 miljoen Vodafone abonnees met een (prepaid of postpaid) data abonnement verkrijgt. De uitkomsten van netwerkstatistieken worden niet minder representatief voor het Vodafone abonneebestand wanneer de gegevens van die ene specifieke individuele betrokkene niet worden meegenomen.

Het CBP neemt verder in aanmerking dat om trends in gebruikersverkeer te identificeren voor netwerkplanning (forecasting en dimensionering), de persoonsgegevens kunnen worden geaggregeerd naar gebruikersgroepniveau en/of netwerkelement en onomkeerbaar worden ontdaan van persoonsidentificerende kenmerken. Niet valt in te zien waarom Vodafone voor (lange termijn) forecasting trends op individueel gebruikersniveau moet volgen. Vodafone geeft in haar zienswijze 1 zelf aan alleen geaggregeerde gegevens nodig te hebben om de benodigde informatie te hebben/(kunnen) krijgen over de netwerkbelasting: *"[VERTROUWELIJK]."*<sup>409</sup>

Het CBP verwijst hierbij ook naar het arrest van het Hof van Justitie van de EG van 16 december 2008, waaruit volgt dat indien het doel de vergaring van statistische gegevens is, het verzamelen en bewaren van gegevens op naam niet is toegelaten.<sup>410</sup>

Er zijn daarnaast meerdere mogelijkheden, en minder ingrijpende middelen, om hetzelfde resultaat te bereiken. Bijvoorbeeld, door (apparatuur die in staat is om) de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren in niet-persistent (werk)geheugen. Mogelijkheden in dat verband zijn onder andere (i)

---

<sup>408</sup> Idem, randnummer 98.

<sup>409</sup> Idem, randnummer 90.

<sup>410</sup> HvJ EG 16 december 2008, EHRC 2009, 23 (LJN: BG7811; Huber).

het (laten) aanpassen van de configuratie-instellingen op bestaande data-analyse apparatuur, zodat de gegevens onmiddellijk na het verzamelen worden verwijderd uit de verkregen dataset, (ii) het (doen) vervangen van thans in gebruik zijnde data-analyse apparatuur door apparatuur die in staat is om de gegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren (in niet-persistent (werk)geheugen) of (iii) het toevoegen van een zogeheten privacy filter (al dan niet op een ander of afzonderlijk apparaat) om de gegevens onmiddellijk na het verzamelen onomkeerbaar te anonimiseren.

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

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat het noodzakelijk is om de bestemmingen (B-nummers) van het internetverkeer te herkennen, net als bij telefonie, om per dienst te kunnen factureren.<sup>411</sup>

**Reactie CBP:** Door de beëindiging van de dienstvoorwaarden BloX bestaat er voor Vodafone geen noodzaak om per klant verschillende internetbestemmingen apart te factureren. Er is daarom geen noodzaak voor Vodafone om verschillende bestemmingen op internet te herkennen voor factureringsdoeleinden. Dit nog los van de toelaatbaarheid daarvan na de inwerkingtreding van artikel 7.4a Tw (nieuw) over netneutraliteit per 1 januari 2013.

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

#### *Technische alternatieven*

**Zienswijze 1 Vodafone:** Vodafone betwist in haar zienswijze 1 dat het mogelijk is om de persoonsgegevens onmiddellijk te anonimiseren en hetzelfde doeleinde te bereiken met minder ingrijpende middelen. *"Het bijplaatsen van apparatuur of uitzetten van functionaliteiten, zoals door het CBP lijkt te worden gesuggereerd (daargelaten de noodzaak daarvoor) betekent - kort gezegd - het toevoegen van een vertragende factor in het systeem die met kostbare, extra rekenkracht (processoren) en met extra energielasten zal moeten worden gecompenseerd (voor zover al mogelijk)."*<sup>412</sup>

Ten aanzien van de [VERTROUWELIJK: apparatuur] schrijft Vodafone: *"Toepassing van het door het CBP bij wijze van alternatief gepresenteerde systeem leidt tot onmiddellijke congestie in het gehele netwerk van Vodafone. Het leidt tevens ertoe dat klanten van Vodafone niet meer op individuele basis kunnen worden geholpen."*<sup>413</sup> En: *"Het CBP moet bewijzen dat er een minder ingrijpende (doch wel effectieve) maatregel*

---

<sup>411</sup> Zienswijze 1 Vodafone, randnummer 91.

<sup>412</sup> Idem, randnummer 28.

<sup>413</sup> Idem, randnummer 44.

*bestaat: dit vereist artikel 3:2 Awb, mede gezien in het licht van de onschuldpresumptie.*"<sup>414</sup>

Vodafone benadrukt dat zij *"technisch niet in staat is om de ruwe data van de [VERTROUWELIJK: apparatuur] te benaderen"* en dat alleen onomkeerbaar geanonimiseerde en geaggregeerde gegevens voor Vodafone beschikbaar zijn.<sup>415</sup>

Ten aanzien van de [VERTROUWELIJK: apparatuur] schrijft Vodafone: *"Vodafone moet snelheden van dataverkeer leveren die klanten van haar verwachten en mogen verwachten. (...). Zonder netwerkbeheer zal Vodafone met klachten, nakomingsvorderingen en opzeggingen worden geconfronteerd. Zónder de [VERTROUWELIJK: apparatuur], of na een anonimisering zoals in het citaat gesuggereerd, kan die afhandeling van mobiele datacommunicatiediensten niet plaatsvinden. Onomkeerbaar anonimiseren is derhalve geen werkbare optie."*<sup>416</sup>

Daarnaast schrijft Vodafone: *"Het is niet aan het CBP om op detailniveau technische maatregelen voor te schrijven. Het CBP dient slechts de grenzen van de wet te bewaken."*<sup>417</sup>

**Reactie CBP:** Het is (inderdaad) niet aan het CBP om zich op detailniveau in te laten met de door Vodafone te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch alternatief voor te schrijven). Het is aan Vodafone om onrechtmatige toepassingen van de data-analyse techniek te voorkomen. In dat verband spelen het proportionaliteits- en subsidiariteitsvereiste een rol (oftewel, is de inbreuk op de belangen van de bij de verwerking betrokkenen evenredig in verhouding tot het met de verwerking te dienen doel en kan het doeleinde niet anderszins of met minder ingrijpende middelen worden bereikt). De voorgaande voorbeelden van technische alternatieven in dit Conceptrapport definitieve bevindingen worden gebruikt om aan te tonen dat er andere mogelijkheden, en minder ingrijpende middelen zijn, om hetzelfde resultaat te bereiken. Hieruit volgt dat de huidige wijze van verwerken van persoonsgegevens op individueel persoonsniveau niet 'noodzakelijk' en 'in overeenstemming met het subsidiariteitsbeginsel' is. Het CBP heeft hiervoor in dit Conceptrapport definitieve bevindingen tevens vastgesteld dat om trends in gebruikersverkeer te identificeren, voor netwerkplanning (forecasting), de persoonsgegevens kunnen worden geaggregeerd naar gebruikersgroepniveau en/of netwerkelement en onomkeerbaar worden ontdaan van persoonsidentificerende kenmerken. Hieruit volgt dat de huidige wijze van verwerken van persoonsgegevens op individueel persoonsniveau ook niet 'noodzakelijk' en 'proportioneel' is.

De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat een alternatief voor de door Vodafone ingezette data-analysetools dat ervoor zorgt dat verkeersgegevens direct onomkeerbaar worden geanonimiseerd op dit moment

---

<sup>414</sup> Idem, randnummer 45.

<sup>415</sup> Idem, randnummer 46.

<sup>416</sup> Idem, randnummer 72.

<sup>417</sup> Idem, randnummer 28.

proportioneel is (de zienswijze 2 van Vodafone heeft ten aanzien van de verwerking via de [VERTROUWELIJK: apparatuur] en de [VERTROUWELIJK: apparatuur] wel geleid tot (gedeeltelijke) aanpassing van de conclusies in het Rapport definitieve bevindingen).

**Zienswijze 1 Vodafone:** Vodafone betwist, zoals vermeld, dat anonimiseren (van gegevens verkregen met de [VERTROUWELIJK: apparatuur]) een werkbare optie is.<sup>418</sup>

**Reactie CBP:** Het is, zoals vermeld, niet aan het CBP om zich op detailniveau in te laten met de door Vodafone te gebruiken data-analyse apparatuur, toepassingen en instellingen (dat wil zeggen: om een bepaald technisch alternatief voor te schrijven). Het is aan Vodafone om onrechtmatige toepassingen van de data-analyse techniek te voorkomen. Op Vodafone rust de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer van de betrokkenen te vermijden dan wel zo beperkt mogelijk te houden. Gegevensverwerking is blijkens artikel 8, onder f, van de Wbp alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook ‘noodzakelijk’ is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke.<sup>419</sup> Vodafone heeft niet aannemelijk gemaakt dat het gebruiken, vastleggen en bewaren van de persoonsgegevens noodzakelijk is op individueel persoonsniveau, althans geaggregeerd per abonnee en dat netwerkplanning in redelijkheid *niet* op een andere, voor de betrokkenen minder nadelige wijze kan worden verwezenlijkt. Het enkele feit dat Vodafone niet bekend is met andere technische oplossingen (die direct toepasbaar zijn) binnen haar mobiele netwerk maakt niet dat de verwerking van persoonsgegevens zoals die thans door Vodafone plaatsvindt proportioneel en subsidiair is.

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

---

<sup>418</sup> Idem, randnummers 44 en 72.

<sup>419</sup> *Kamerstukken II 1998/99, 25 892, nr. 13, p. 6: “Overigens wijzen wij erop dat alleen een gerechtvaardigd belang niet voldoende is. Gegevensverwerking is blijkens artikel 8, onder f, alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook «noodzakelijk» is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke.”*



### *Wettelijke plicht*

**Zienswijze 1 Vodafone:** In haar zienswijze 1 schrijft Vodafone voorts: *"Het CBP gaat ten onrechte niet in "op wettelijke verplichtingen zoals 11.3 Tw en artikel 14.6 Tw (en de Regeling voorbereiding buitengewone omstandigheden 2007). Onzorgvuldig is dan ook de volstrekt niet nader onderzochte stelling dat artikel 8 sub c Wbp niet als grondslag aan de orde is."*<sup>420</sup> Tevens verwijst Vodafone naar aanstaande wijzigingen van de Tw, met name 7.4a en 11.2a Tw. *"Uitgangspunten daarbij zijn ondermeer dat een regulier verkeersmanagement mogelijk moet blijven. Volgens de Memorie van Antwoord staat artikel 7.4a er niet aan in de weg dat een aanbieder kijkt of hij te maken heeft met een VOIP dienst of een e-maildienst om deze vervolgens (om) de voor de hand liggende redenen bij congestie verschillend te behandelen."*<sup>421</sup>

**Reactie CBP:** Vodafone schrijft, zo begrijpt het CBP, dat nodig is dat gebruik wordt gemaakt van netwerkmanagement-toepassingen, waarmee de verschillende verkeersstromen op het netwerk op het niveau van de individuele abonnees in kaart worden gebracht, om aan verschillende wettelijke verplichtingen te kunnen voldoen. Indien en voor zover Vodafone zich ten aanzien van dit doeleinde beroept/wenst te beroepen op de grondslag wettelijke plicht (artikel 8, aanhef en onder c, van de Wbp), een verplichting die zou voortvloeien uit een of meerdere van de hieronder genoemde wetsartikelen<sup>422</sup>, stelt het CBP het volgende vast.

### Ad artikel 11.3 van de Tw (passende technische en organisatorische maatregelen)

Artikel 11.3 van de Tw is onvoldoende specifiek om ter zake van dit subdoeleinde een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en (de uitvoering van) de wettelijke verplichting.

### Ad artikel 14.6 van de Tw (voorbereiding buitengewone omstandigheden)

Artikel 14.6 van de Tw en de bijbehorende Regeling voorbereiding buitengewone omstandigheden Telecommunicatiewet<sup>423</sup> betreffen, kort samengevat, de mogelijkheid dat de minister van Economische Zaken, Landbouw en Innovatie, in samenspraak met de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie verplichtingen kan opleggen aan een aanbieder van openbare vaste en mobiele spraaktelefonie en van toegang tot breedbandinternet om zich voor te bereiden op elektronisch transport van gegevens in buitengewone omstandigheden, zoals bijvoorbeeld oorlog. Deze bepaling is evenmin voldoende specifiek om ter zake een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken.

---

<sup>420</sup> Zienswijze 1 Vodafone, p. 27.

<sup>421</sup> Idem.

<sup>422</sup> Het CBP heeft de toepassing van de hieronder genoemde wetsartikelen voorgelegd aan OPTA en Agentschap Telecom in het kader van het Samenwerkingsprotocol CBP-OPTA onderscheidenlijk de Samenwerkingsovereenkomst Agentschap Telecom-CBP van beide toezichthouders. OPTA (thans: de ACM) en Agentschap Telecom stemmen elk voor zover zij ter zake de bevoegde toezichthouder zijn in met de voorgelegde toepassing van deze wetsartikelen.

<sup>423</sup> *Scrt.* 2011, 5400.

Ad artikel 22, derde lid, van de gewijzigde Universeledienstrichtlijn (geïmplementeerd in artikel 7.4a, vijfde lid, van de Tw (nieuw): kwaliteit van de dienst), artikel 7.4a, eerste lid, van de Tw (nieuw) (netneutraliteit) en artikel 23 van de gewijzigde Universeledienstrichtlijn (zoals geïmplementeerd in artikel 11a.1 van de Tw (nieuw): beschikbaarheid van diensten) en artikel 11a.2 van de Tw (nieuw)

Artikel 7.4a van de Tw treedt in werking op 1 januari 2013.

Artikel 7.4a, vijfde lid, van de Tw (nieuw) vormt een implementatie van artikel 22, derde lid, van de gewijzigde Universeledienstrichtlijn. Voor zover deze bepaling de *mogelijkheid* biedt minimumkwaliteitseisen te stellen aan de dienstverlening zodat een achteruitgang van de dienstverlening of een belemmering of vertraging van het verkeer via internet kan worden voorkomen, geldt dat daarmee op zichzelf geen sprake is van een wettelijke verplichting. Zulke minimumkwaliteitseisen zijn (nog) niet gesteld (bij of krachtens algemene maatregel van bestuur). Er is dus geen verplichting, opgenomen in een wettelijke bepaling, die op Vodafone rust en waarvan de verwerking met toepassing van data-analyse technieken van (gevoelige) persoonsgegevens op persoonsniveau een noodzakelijk uitvloeisel is.

Artikel 7.4a, eerste lid, van de Tw (nieuw), regelt de verplichting voor aanbieders om netneutraal te handelen, met daarop een aantal uitzonderingen (bijvoorbeeld om de gevolgen van congestie te beperken, waarbij gelijke soorten verkeer gelijk worden behandeld, of ter uitvoering van een wettelijk voorschrift of rechterlijk bevel). Indien en voor zover een van de uitzonderingssituaties van toepassing is, betekent dit dat de netneutraliteitsverplichting niet geldt. Artikel 7.4a van de Tw (nieuw) is nog niet in werking getreden. Daar komt bij dat de uitzonderingen op de netneutraliteitsverplichting als geformuleerd in dit artikel 7.4a, eerste lid, van de Tw (nieuw) geen wettelijke verplichting vormen om, ter invulling van zo'n uitzonderingssituatie, met toepassing van data-analyse technieken (gevoelige) persoonsgegevens op persoonsniveau te verwerken. De uitzonderingen bepalen alleen iets over de toelaatbaarheid van niet-netneutraal handelen. In dit verband wijst het CBP erop dat in artikel 7.4a, eerste lid, onder d, van de Tw een afzonderlijke uitzondering is geregeld op de netneutraliteitsverplichting "*ter uitvoering van een wettelijk voorschrift (...)*": de wetgever heeft dus bedoeld dat de wettelijke verplichting moet voortvloeien uit een andere wettelijke bepaling dan het netneutraliteitsartikel. Er is dus geen verplichting, opgenomen in een wettelijke bepaling, waarvan de gegevensverwerking een noodzakelijk uitvloeisel is.

Datzelfde geldt ten aanzien van artikel 11a.1 en 11a.2 van de Tw (nieuw) over de veiligheid en integriteit van netwerken en diensten en de meldplicht voor veiligheidsinbreuken en het verlies van integriteit. Artikel 11a.1 van de Tw, over passende technische en organisatorische maatregelen om de risico's voor de veiligheid en de integriteit van netwerken en diensten te beheersen, is voor het overige ook onvoldoende specifiek om voor dit subdoeleinde ter zake een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er

bestaat geen evident verband tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.<sup>424</sup>

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

#### *Video-optimalisatie*

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat video-optimalisatie een vorm is van verkeersbeheer, *"wat onder de Tw wordt geacht te zijn afgeleid van het factureringsdoeleinde (...). Ook voor deze vorm van verkeersbeheer bestaat dus een uitdrukkelijke wettelijke grondslag (op basis van de Tw). Daarmee staat vast dat aan de Wbp is voldaan, conform het eerder gestelde. Er is sprake van noodzakelijkheid om een overeenkomst waarbij de betrokkene partij is, uit te voeren; dus ook in de zin van artikel 8 onder b Wbp, of subsidiair artikel 8 sub f Wbp (noodzakelijk voor een provider om zijn reguliere activiteiten te kunnen verrichten)."*<sup>425</sup> Aanvullend schrijft Vodafone: *"Video-optimalisatie is in het belang van de eindgebruiker; als dit niet wordt geboden werkt het netwerk langzamer, zal het bekijken van videobeelden vaker vastlopen en is de klant bovendien duurder uit. (...) Redelijkerwijs valt dan ook niet in te zien waarom een klant tegen video-optimalisatie bezwaar zou kunnen hebben (...)"*<sup>426</sup>

**Reactie CBP:** Ten aanzien van de gegevens over het dataverkeer (niet zijnde communicatie, zoals URL's) geldt dat artikel 8 van de Wbp van toepassing is, 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. Op grond van artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw is de verwerking van niet-geanonimiseerde verkeersgegevens toelaatbaar indien deze noodzakelijk is voor 'verkeersbeheer' (oftewel, activiteiten ter verbetering van de netwerk performance of de dienstverlening van de mobiele aanbieder). Vodafone heeft verklaard dat de verwerking van persoonsgegevens noodzakelijk is om bijvoorbeeld video's met de gewenste snelheid te kunnen leveren én om de abonnee geld te besparen voor onnodig dataverkeer.<sup>427</sup> Vodafone heeft aannemelijk gemaakt dat hieruit volgt dat de verwerking van de persoonsgegevens noodzakelijk is voor Vodafone om bijvoorbeeld haar reguliere bedrijfsactiviteiten te kunnen verrichten. Uit het voorgaande blijkt dat Vodafone een grondslag voor deze verwerking van persoonsgegevens zou kunnen hebben onder artikel 11.5, eerste en tweede jo. vijfde lid, van de Tw. Zo'n grondslag correspondeert met de grondslagen uitvoering van een overeenkomst en/of een noodzaak (artikel 8, aanhef en onder b en/of f, van de Wbp).

---

<sup>424</sup> Het CBP heeft eveneens gekeken naar artikel 11.2 van de Tw (zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer. Deze bepaling is onvoldoende specifiek om voor dit doeleinde ter zake een verplichting aan te nemen om met toepassing van data-analyse technieken de (gevoelige) persoonsgegevens op persoonsniveau te verwerken, althans er bestaat geen evident verband tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting.

<sup>425</sup> Zienswijze 1 Vodafone, randnummer 116.

<sup>426</sup> Idem, randnummer 117.

<sup>427</sup> Idem.

Vodafone inspecteert en analyseert bij de toegepaste video-optimalisatie alle URL's van de video's, om realtime technische compressie op video's en webpagina's toe te kunnen passen, tijdens de internetssessie van een abonnee. Ten aanzien van URL's geldt dat (richtlijnconforme uitleg van) artikel 5, eerste lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw (nieuw) dat in werking treedt op 1 januari 2013) een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen.

Ten aanzien van de de grondslagen uitvoering van een overeenkomst en/of een noodzaak (artikel 8, aanhef en onder b en/of f, van de Wbp) geldt het volgende.

De verwerking van persoonsgegevens is toelaatbaar indien deze 'noodzakelijk' is voor de uitvoering van een overeenkomst of, bij de behartiging van het gerechtvaardigd belang, als het belang op bescherming van de persoonlijke levenssfeer van individuele betrokkenen niet prevaleert (proportionaliteits- en subsidiariteitstoets).

Vodafone heeft aannemelijk gemaakt dat de verwerking van de persoonsgegevens (tevens communicatie) noodzakelijk is voor Vodafone om bijvoorbeeld haar reguliere bedrijfsactiviteiten te kunnen verrichten. Op basis van het beschikbare onderzoeksmateriaal, waaruit blijkt dat Vodafone geen inhoud van het dataverkeer opslaat (bijvoorbeeld download URL's die iets (kunnen) zeggen over individueel videokijkgedrag), is de inbreuk op de belangen van betrokkenen niet onevenredig in verhouding tot het met de verwerking te dienen doel.

Uit het voorgaande blijkt dat Vodafone in elk geval een grondslag voor deze verwerking van persoonsgegevens heeft onder artikel 8, aanhef en onder f, van de Wbp.

De zienswijze 1 van Vodafone heeft op dit punt wel geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat het CBP op basis van het beschikbare onderzoeksmateriaal ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens geen overtreding heeft geconstateerd van (artikel 11.5 van de Tw jo.) artikel 8 van de Wbp.

*Firewalls, spamfilters en virusscanners*

**Zienswijze 1 Vodafone:** In haar zienswijze 1 schrijft Vodafone ten aanzien van firewalls, spamfilters en virusscanners dat *"naar haar oordeel artikel 8 aanhef en sub b (uitvoering van een overeenkomst) een grondslag voor de verwerking vormt, en minst genomen een gerechtvaardigd belang."*<sup>428</sup>

**Reactie CBP:** Ten aanzien van de spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer geldt dat artikel 8 van de Wbp van toepassing is, zij het dat (richtlijnconforme uitleg van) artikel 5, eerste lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw (nieuw) een nadere begrenzing/inperking geeft van de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen. Op grond van artikel 5, eerste lid, van de e-Privacyrichtlijn is het af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende

---

<sup>428</sup> Idem, randnummer 118.

verkeersgegevens door een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst verboden indien de betrokken abonnees daarin niet hebben toegestemd, tenzij het bij wet is toegestaan.

Het CBP merkt op dat voor zover artikel 11.3 van de Tw verplicht tot het gebruik van firewalls, (uitgaande) spamfilters en virusscanners (zie hieronder), geldt dat de grondslag voor de verwerking van persoonsgegevens, tevens communicatie moet worden gevonden in artikel 8 van de Wbp.

De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat het CBP op basis van het beschikbare onderzoeksmateriaal ten aanzien van de in deze paragraaf besproken verwerking van persoonsgegevens geen overtreding heeft geconstateerd van artikel 8 van de Wbp.

*Behandeling van verzoeken om inlichtingen van klanten*

**Zienswijze 1 Vodafone:** In haar zienswijze 1 voegt Vodafone toe dat ook uitvoering van de overeenkomst en minst genomen, een gerechtvaardigd belang, grondslagen van de verwerking vormen.<sup>429</sup>

**Reactie CBP:** De door Vodafone genoemde grondslagen kunnen van toepassing zijn als het om persoonsgegevens, tevens verkeersgegevens gaat. Ten aanzien van persoonsgegevens, tevens inhoudelijke communicatiegegevens zoals hostnames, is toestemming de enige mogelijke grondslag. Dit wordt in dit Conceptrapport definitieve bevindingen uitgewerkt en gemotiveerd (de gegevensverwerking is niet noodzakelijk ten behoeve van de goede werking van een openbaar telecommunicatienetwerk).

De zienswijze 1 van Vodafone heeft op dit punt geleid tot aanpassing van de bevindingen en conclusies in het Conceptrapport definitieve bevindingen dat nu van (voorafgaande) ondubbelzinnige toestemming niet is gebleken, Vodafone geen grondslag heeft voor de verwerking van de persoonsgegevens voor het behandelen van verzoeken om inlichtingen van klanten.

**Zienswijze 1 Vodafone:** In haar zienswijze 1 geeft Vodafone aan dat de gegevensverwerking voor het behandelen van (individuele) klantklachten niet expliciet in de leveringsvoorwaarden staat. *"De overeenkomst tussen Vodafone en consument bestaat niet alleen uit wat zij met elkaar zijn overeengekomen in het contract (...), maar ook wat uit de aard van het contract, de gewoonte en redelijkheid en billijkheid voortvloeit (art. 6:248 lid 1 Bw)."*<sup>430</sup>

**Reactie CBP:** De zienswijze 1 van Vodafone heeft op het punt van de door Vodafone verstrekte informatie geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

*Prepaidverkeer*

---

<sup>429</sup> Idem, randnummer 119.

<sup>430</sup> Idem, randnummer 68.

**Zienswijze 1 Vodafone:** "[VERTROUWELIJK]. Aldus valt deze betrokken verwerking eveneens onder 11.5 Tw en is er ook overigens sprake van noodzakelijkheid ter uitvoering van een overeenkomst waarbij de betrokkene partij is in de zin van artikel 8 sub b Wbp."<sup>431</sup>

**Reactie CBP:** [VERTROUWELIJK]

De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen dat een alternatief voor het door Vodafone ingezette data-analyse apparaat, zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer waarmee de prepaid abonnee een betalingswebsite kan bezoeken, op dit moment proportioneel is (de zienswijze 2 van Vodafone heeft op dit punt wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen).

**Zienswijze 1 Vodafone:** "[VERTROUWELIJK]."<sup>432</sup>

**Reactie CBP:** Het CBP heeft in het Conceptrapport definitieve bevindingen gemotiveerd vastgesteld dat er technische alternatieven zijn, zoals het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een betalingswebsite kan bezoeken.

De zienswijze 1 van Vodafone heeft op het punt van de inzet van data-analyse technieken voor de facturering van prepaidverkeer niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft op dit punt wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen). De inzet van data-analyse technieken voor de facturering van MMS-verkeer is naar aanleiding van de zienswijze 1 van Vodafone buiten de scope van dit onderzoek verklaard.

*Verdere verwerking*

**Zienswijze 1 Vodafone:** Vodafone schrijft in haar zienswijze 1 dat de gegevens na anonimisering geen persoonsgegevens meer zijn en dat het daarom het CBP aan wettelijke grondslag ontbreekt om ten aanzien van de geanonimiseerde verzameling op te treden.

**Reactie CBP:** Het CBP heeft vastgesteld in dit Conceptrapport definitieve bevindingen dat Vodafone persoonsgegevens verzamelt en deze daarna anonimiseert. Anonimiseren is een vorm van gegevensverwerking waarvoor een grondslag is vereist in artikel 8 van de Wbp.

De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen dat nu Vodafone niet mag beschikken over de (achterliggende) persoonsgegevens, het Vodafone ook niet is toegestaan om deze gegevens naderhand (in concreto, na een uur) te anonimiseren om (in geanonimiseerde vorm) verder te verwerken voor het vaststellen van de business strategie (de zienswijze 2 van Vodafone heeft op dit punt wel geleid tot aanpassing van de conclusies in het Rapport definitieve bevindingen).

---

<sup>431</sup> Idem, randnummer 120.

<sup>432</sup> Idem, randnummers 122-123.

## Doeleinden

**Zienswijze 1 Vodafone:** *"Vodafone betwist dat de doeleinden voor de gegevensverwerkingen niet welbepaald en uitdrukkelijk zouden zijn omschreven. (...) De verwerking van persoonsgegevens (...) zijn namelijk allen noodzakelijk voor de uitvoering van de overeenkomst die het gevolg is van de aansluiting om telecommunicatiediensten van Vodafone te gebruiken en dienen voorts ter optimalisatie van haar dienstverlening (gerechtvaardigd belang)."*<sup>433</sup>

**Reactie CBP:** In de wetsgeschiedenis bij artikel 7 van de Wbp is over het begrip 'uitdrukkelijk omschreven' opgemerkt: *"Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen. In de gevallen dat hij op grond van artikel 29 van de melding is vrijgesteld, geldt het doel dat bij algemene maatregel van bestuur is omschreven op grond van artikel 29 tweede lid, onder a."*<sup>434</sup> Hieruit volgt dat de wetgever heeft bedoeld dat het criterium in dit geval is of Vodafone de doeleinden waarvoor zij persoonsgegevens verwerkt, heeft omschreven bij de meldingen die zij heeft gedaan. Uit de melding blijkt niet voor welke verschillende doeleinden Vodafone persoonsgegevens verzamelt en verwerkt. Uit de doeleinden 'voorkomen van fraude en misbruik', dan wel 'bevorderen van de beveiliging van Vodafone's organisatie en haar netwerk' kan niet worden opgemaakt dat Vodafone persoonsgegevens uit de inhoud van bestanden en e-mails verwerkt om spam, virussen en malware tegen te gaan en te verwijderen. Uit het doeleinde 'optimalisatie van de dienstverlening' kan niet worden opgemaakt dat Vodafone video-optimalisatie toepast als abonnees video's op internet bekijken.

In de concept gewijzigde melding die Vodafone bij haar zienswijze 1 heeft gevoegd, wordt het doel van verwerking 'sluiten en uitvoeren van de overeenkomst' uitgebreid met een toelichting dat dit tevens factureren betreft, *"waaronder begrepen het factureren van MMS-verkeer en debiteurenadministratie alsmede verkeer- en netwerkmanagement, waaronder begrepen transporteren van het verkeer van prepaidklanten naar opwaardeersites en videocompressie, om het gebruik van het netwerk te kunnen analyseren, de continuïteit, beveiliging en integriteit van het netwerk te waarborgen en te bevorderen, (gevolgen van) congestie te beperken en fraude en hoog verbruik te detecteren (onder andere voor bill-shock preventie)."*

Vodafone stelt tevens voor om het doeleinde 'Klachtoplossing, afhandeling verzoeken om inlichtingen van klanten/gebruikers en berechting en beslissing van geschillen' toe te voegen aan de melding.

Met de concept gewijzigde melding wordt het *"transporteren van het verkeer van prepaidklanten naar opwaardeersites"* omschreven. Tevens wordt videocompressie genoemd, onder facturering. De overige subdoeleinden van verkeersbeheer zijn onvolledig en onvoldoende duidelijk omschreven in de doelomschrijving van de concept gewijzigde melding, namelijk: *"om het gebruik van het netwerk te kunnen analyseren"*. Hieruit wordt niet, althans onvoldoende, duidelijk dat Vodafone data-analysetechnieken toepast op persoonsgegevens (vaak tevens communicatie respectievelijk verkeersgegevens) op abonnee niveau.

---

<sup>433</sup> Idem, randnummer 126.

<sup>434</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 79.

Met de concept gewijzigde melding wordt het doeleinde klachtprocessing, afhandeling verzoeken om inlichtingen van klanten/gebruikers en berechting en beslissing van geschillen omschreven.

Dit geldt tevens voor het doeleinde 'beveiliging'. Uit de zinsnede (om) "*de continuïteit, beveiliging en integriteit van het netwerk te waarborgen en te bevorderen*" kan niet worden opgemaakt dat Vodafone data-analysetechnieken toepast op de inhoud van gedownloade bestanden en e-mails voor spam-, virus- en malwarefiltering.

Doordat Vodafone de hierboven genoemde doeleinden waarvoor zij persoonsgegevens verwerkt niet, althans onvolledig en onvoldoende duidelijk omschrijft in de concept gewijzigde melding, worden ook na het doorvoeren van die wijzigingen de door Vodafone verzamelde persoonsgegevens niet voor uitdrukkelijk omschreven doeleinden verzameld en handelt Vodafone in strijd met artikel 7 van de Wbp.

De zienswijze 1 van Vodafone heeft op het punt van het begrip 'uitdrukkelijk omschreven' doeleinden geleid tot verduidelijking en aanpassing/aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

### Informatieplicht

**Zienswijze 1 Vodafone:** Vodafone verwijst ten aanzien van de verstrekte informatie in haar zienswijze ook naar de artikelen 6.3 en artikel 6.6 van de Algemene Voorwaarden.<sup>435</sup>

**Reactie CBP:** Deze artikelen luiden, voor zover voor dit onderzoek van belang:

6.3 "*Vodafone spant zich in om het Vodafone Netwerk zodanig in te richten, dat de Diensten zo min mogelijk door beperkingen en verstoringen worden beïnvloed.*"

6.6 "*Vodafone onderhoudt het Vodafone netwerk op een continue basis en streeft er naar om het Vodafone Netwerk op een kwalitatief hoogstaand niveau te laten functioneren.*"

De zienswijze 1 van Vodafone heeft op dit punt geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

**Zienswijze 1 Vodafone:** Bij haar zienswijze 1 heeft Vodafone een concept wijziging van het Privacy Statement gevoegd.

**Reactie CBP:** De zienswijze 1 van Vodafone heeft op dit punt geleid tot aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op

---

<sup>435</sup> Zienswijze 1 Vodafone, randnummer 103.



dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft wel geleid tot gedeeltelijke aanpassing van de conclusies in het Rapport definitieve bevindingen).

**Zienswijze 1 Vodafone:** In haar zienswijze 1 schrijft Vodafone: *"De Privacyrichtlijn 95/46/EG noemt als voorbeelden van nadere informatie: gegevenscategorieën, (categorieën van) ontvangers, het bestaan van een recht op toegang tot zijn eigen persoonsgegevens en op rectificatie van deze gegevens. Deze informatie wordt vermeld in het Privacy Statement. Nadere details hoeven niet worden vermeld."* Vodafone bestrijdt specifiek dat zij verplicht zou zijn abonnees te informeren over de bewaartermijn(en). De privacyrichtlijn 95/46/EG zou hiertoe niet verplichten.<sup>436</sup>

**Reactie CBP:** Artikel 11, eerste lid, onder c, van de Privacyrichtlijn geeft *voorbeelden* van nadere informatie. Het betreft geen uitputtend overzicht. Welke nadere informatie vereist is, hangt op grond van artikel 34, derde lid van de Wbp af van de aard van de gegevens, de omstandigheden waaronder zij worden verkregen en het gebruik dat ervan wordt gemaakt. De omstandigheden in dit onderzoek moeten mede in het licht worden gezien van de maatschappelijke ophef die medio 2011 in Nederland is ontstaan over de aankondiging van onder meer Vodafone om diensten apart in rekening te willen gaan brengen. Die ophef heeft er (mede) toe geleid dat de Tweede Kamer per amendement een specifieke netneutraliteitsbepaling heeft opgenomen in de Telecommunicatiewet.<sup>437</sup>

Bij haar zienswijze heeft Vodafone een concept wijziging van haar Privacy Statement toegevoegd. In dit Privacy Statement wordt een toelichting gegeven op het gebruik van *"internetgegevens en informatie over het hoe het netwerk en jouw telefoon in combinatie met het netwerk werkt."* In de voorgestelde wijziging worden de doeleinden verkeersbeheer en facturering, klachtafhandeling, facturering van MMS-berichten en bezoek aan betaalsites door prepaidklanten waarvan het tegoed verbruikt is, toegelicht. Onder verkeersbeheer wordt video-optimalisatie als volgt beschreven: *"Zo kunnen we een video bijvoorbeeld in delen door het netwerk sturen."* Vodafone schrijft verder: *"Ook kijken we naar het totale verkeer van onze klanten, dit doen we anoniem, om bepaalde verkeerstrends te ontdekken (...)"*

Het CBP heeft vastgesteld in dit Conceptrapport definitieve bevindingen dat Vodafone eerst persoonsgegevens, tevens communicatie verwerkt, alvorens te anonimiseren. Hieruit volgt dat de zinsnede uit de privacyverklaring dat Vodafone anoniem kijkt naar het totale verkeer als feitelijk onjuist moet worden aangemerkt, althans onvolledig en onvoldoende duidelijk is.

Vodafone informeert betrokkenen via de concept wijzigingen voorts niet over de categorieën van verwerkte persoonsgegevens, tevens communicatie zoals hostnames, URL's en app/protocol/service en spam-, virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

---

<sup>436</sup> Idem, randnummer 129.

<sup>437</sup> Zie bijvoorbeeld: NRC Handelsblad, Nieuwe Telecomwet aangenomen door Eerste Kamer, 8 mei 2012, URL: <http://www.nrc.nl/nieuws/2012/05/08/wet-netneutraliteit-aangenomen-door-eerste-kamer/>.

Bovendien ontbreekt informatie over de bewaartermijnen voor de verschillende doeleinden.

Ook als Vodafone de concept wijzigingen doorvoert, duurt de overtreding van artikel 34 van de Wbp in zoverre voort.

De zienswijze 1 van Vodafone heeft op dit punt geleid tot aanpassing en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen (de zienswijze 2 van Vodafone heeft wel geleid tot gedeeltelijke aanpassing van de conclusies in het Rapport definitieve bevindingen).

### Meldingsplicht

**Zienswijze 1 Vodafone:** Vodafone brengt in haar zienswijze 1 naar voren dat ze onverplicht bereid is de melding uit te breiden en daartoe een voorstel aan het CBP zal doen. Een concept is als bijlage bij de zienswijze gevoegd.<sup>438</sup>

In haar zienswijze schrijft Vodafone (ver) dat er geen verplichting bestaat om de melding zodanig specifiek te laten zijn dat de inzet van data analyse technieken met naam en toenaam in de melding zou moeten worden opgenomen.<sup>439</sup>

**Reactie CBP:** Het CBP betoogt niet dat Vodafone is gehouden het gebruik van data-analyse te omschrijven *als doeleinde* bij de melding die zij heeft gedaan. Het CBP heeft hierboven vastgesteld dat de doeleinden van de gegevensverwerking die betrekking hebben op de verwerking van persoonsgegevens bij de inzet van data-analyse technieken in haar mobiele netwerk voor het doeleinde verkeersbeheer onvoldoende specifiek zijn.

De zienswijze 1 van Vodafone heeft op dit punt geleid tot aanpassing en aanvulling van de feitelijke bevindingen in het rapport. De zienswijze 1 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het Conceptrapport definitieve bevindingen.

---

<sup>438</sup> Zienswijze 1 Vodafone, p. 4, randnummers 25 en 132. Bijlage 6 is de concept gewijzigde melding.

<sup>439</sup> Idem, randnummer 132.

Bijlage V Zienswijze 2 Vodafone, met de reactie daarop van het CBP (zoals weergegeven in het rapport definitieve bevindingen, gegroepeerd én aangevuld met in hoeverre de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies van het rapport definitieve bevindingen).

Onzorgvuldig en ondeugdelijk onderzoek dient tot sluiten dossier te leiden

**Zienswijze 2 Vodafone:** Vodafone stelt zich in haar zienswijze 2 op het standpunt dat het onderzoek van het CBP wordt gekenmerkt door onzorgvuldigheid en dat het onderzoek om die reden moet worden beëindigd en dat geen definitief rapport van bevindingen kan worden vastgesteld, laat staan openbaar gemaakt en dat geen sanctie kan worden opgelegd.<sup>440</sup> Vodafone noemt (kort gezegd) de navolgende redenen.

*Scope: onduidelijkheid omtrent de reikwijdte en het onderwerp van onderzoek en de onderzoeksvragen*

Vodafone brengt in haar zienswijze 2 naar voren dat er onduidelijkheid is (geweest) omtrent de reikwijdte en het onderwerp van onderzoek en de onderzoeksvragen. Vodafone wijst erop dat de precieze onderzoeksvragen Vodafone niet gedurende het onderzoek zijn medegedeeld en eerst in het Rapport voorlopige bevindingen waren geformuleerd. Vodafone wijst er verder op dat de reikwijdte (scope) van het onderzoek is aangepast. Vodafone meent dat zij hierdoor is gedwongen om mee te werken aan haar eigen veroordeling, nu haar om zeer veel informatie is gevraagd (die het CBP ook heeft gekregen) zonder dat Vodafone duidelijk is gemaakt in het kader van welke onderzoeksvragen deze informatie is gevraagd en zou worden gebruikt (*fishing expedition*).<sup>441</sup>

Dit geldt temeer daar volgens Vodafone zodra een van de (vermeende) overtredingen (specifiek: de meldingsplicht) punitief kan worden gesanctioneerd (met een bestuurlijke boete), de waarborgen van artikel 6 van het EVRM (onder andere onschuldpresumptie)<sup>442</sup> zich uitstrekken over het gehele onderzoek. Dit gezien de onlosmakelijke verbondenheid van de onderzoeksvragen/het feit dat het CBP constateert dat bepaalde verwerkingen geen geldige grondslag hebben en dus de meldingsplicht is geschonden. Er is ook nooit een cautie gegeven.<sup>443</sup>

Vodafone verzet zich ook overigens tegen de door het CBP gekozen scopebeperking, omdat de scope nogal willekeurig is (schijn van *cherry picking*), bijvoorbeeld het buiten het onderzoek houden van de inzet van data-analyse technieken voor bill shock door data roaming en de facturering van MMS-verkeer. Verder merkt Vodafone op dat het buiten de scope vallen van de gegevensverwerking die verband houdt met de Dienstvoorwaarden Vodafone BloX vanwege de beëindiging/uitfasering daarvan, niet consequent wordt doorgevoerd in het Conceptrapport definitieve bevindingen.<sup>444</sup>

*Hoor en wederhoor, onschuldpresumptie en reformatio in peius*

---

<sup>440</sup> Zienswijze 2 Vodafone, p. 2. Zie ook idem, p. 10-11 en 51.

<sup>441</sup> Idem, p. 2 en 18-19. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 4-5 en 7.

<sup>442</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 3.

<sup>443</sup> Zienswijze 2 Vodafone, p. 3, 11 en 19.

<sup>444</sup> Idem, p. 40 en 54.

Vodafone meent dat het CBP niet (eerst) een Conceptrapport definitieve bevindingen aan haar had mogen voorleggen voor een tweede zienswijze. Dit omdat mogelijk een (punitieve) sanctie kan worden opgelegd en het CBP in de begeleidende brief bij het Rapport voorlopige bevindingen had aangekondigd dat na dit eerste rapport een definitief rapport zou volgen. Het geven van een zienswijze is een verdedigingsrecht (recht van hoor en wederhoor), aldus Vodafone. Het is in strijd met de onschuldpresumptie (artikel 6 van het EVRM) om een zienswijze met kritiek op en weerlegging van voorlopige bevindingen (zowel feitelijk als juridisch) te gebruiken om onderzoek(svragen) aan te scherpen en feiten aan te vullen, laat staan extra overtredingen te constateren.<sup>445</sup>

#### *Rechtszekerheid en artikel 6 van het EVRM*

Volgens Vodafone bevat het Conceptrapport definitieve bevindingen ondanks de zeer omvangrijke hoeveelheid informatie en antwoorden die het CBP van Vodafone heeft gekregen feitelijke onjuist- en onzorgvuldigheden. Het is aan de toezichthouder om de juiste feiten boven tafel te krijgen - in tijd, omvang en gelegenheden begrepen. De rechtszekerheid - en artikel 6 van het EVRM - vereist daarom dat het onderzoek moet worden gesloten (een andere lezing zou leiden tot strijd met het zelfincriminatieverbod).<sup>446</sup>

#### *Fair play-beginsel, onzorgvuldig en in strijd met het zelfincriminatieverbod*

Vodafone geeft in haar zienswijze 2 aan dat het in strijd met het fair play-beginsel, onzorgvuldig en in strijd met het zelfincriminatieverbod is dat het CBP niet in overleg wil treden met haar over de melding en het Privacy Statement - evenals het terugbrengen van bewaartermijnen - en evenmin over het herhaaldelijke aanbod van Vodafone (ook in haar zienswijze 2<sup>447</sup> en reactie op de vordering van het CBP<sup>448</sup>) om in gezamenlijk overleg te overzien hoe eventuele overtredingen zo snel en zo effectief mogelijk kunnen worden beëindigd, of een voorstel ex ante te toetsen (en bestrijdt de motivering van de afwijzing).<sup>449</sup> Dit ook gelet op de zeer hoge kosten van ingrepen in de netwerkarchitectuur en het zware economische tij.<sup>450</sup> Dat geldt temeer daar op overtreding van de meldplicht een punitieve sanctie staat, de Wbp open normen bevat en het gaat om een technische omgeving, waarbij tevens onduidelijkheden bestaan over de toepasselijkheid van de Wbp en de Tw.<sup>451</sup> Er kan dan ook niet worden geconstateerd dat de wet is overtreden als het gaat om bijvoorbeeld de meldplicht.<sup>452</sup>

#### *Toekomstige regelgeving*

In haar zienswijze 2 wijst Vodafone erop dat het CBP kwalificaties geeft over de rechtmatigheid van het gebruik van 'data-analyse technieken' onder nieuwe regelgeving (artikel 7.4a en artikel 11.2a van de Tw (nieuw)), ten aanzien waarvan het CBP (deels) geen bevoegdheden heeft, maar waarvoor bovenal geen enkele noodzaak

---

<sup>445</sup> Idem, p. 2-3, 22 en 67.

<sup>446</sup> Idem, p. 3-4 en 21-22.

<sup>447</sup> Idem, p. 72.

<sup>448</sup> Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 7.

<sup>449</sup> Zie Zienswijze 2 Vodafone, p. 20-21, 37 en 71. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 15.

<sup>450</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 7-8.

<sup>451</sup> Zienswijze 2 Vodafone, p. 4-5. Vgl. ook idem, p. 20.

<sup>452</sup> Idem, p. 72.

of aanleiding bestaat. Vodafone heeft het CBP laten weten alle huidige proposities die niet met die artikelen stroken vóór de inwerkingtreding van de relevante regels te beëindigen c.q. rechtmatig uit te faseren. Het benoemen van de implicaties van deze nieuwe regels is volgens Vodafone tendentiekus en vooringenomen.<sup>453</sup>

#### *Onderzoeks- en motiveringsplicht CBP*

Vodafone brengt in haar zienswijze 2 naar voren dat het onderzoek c.q. Conceptrapport van bevindingen (kort gezegd) onzorgvuldig is voorbereid en ontoereikend is gemotiveerd. Vodafone wijst in dat verband op het volgende.

Volgens Vodafone motiveert het CBP onvoldoende waarom er ten aanzien van bepaalde data-analyse technieken (te weten: de (sub)doeleinden verkeersbeheer en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites) alternatieve, voor de betrokken eindgebruikers vermeend lichtere (dat wil zeggen: minder ingrijpende) maatregelen kunnen worden gebruikt (ten onrechte is ook niet in kaart gebracht wat de gevolgen, bijvoorbeeld voor de netwerkindegriteit en stabiliteit, zouden zijn van zulke alternatieven).<sup>454</sup> Ook is (de verwerking van) de zienswijze 1 van Vodafone in (de inleiding in) het Conceptrapport definitieve bevindingen onvoldoende weergegeven<sup>455</sup> en zou het CBP tegenbewijs van Vodafone niet hebben meegenomen (onder andere een verklaring van de leverancier [VERTROUWELIJK] dat een dergelijke lichtere maatregel niet werkt). Het is aan de toezichthouder om de juiste feiten boven tafel te krijgen en zijn stellingen toereikend te motiveren, met name waar het treffen van maatregelen ingrijpende gevolgen heeft voor de bedrijfsvoering en in een context waarin een geconstateerde overtreding tot sanctieoplegging kan leiden.<sup>456</sup> Vodafone merkt verder op dat het 'feit van algemene kennis' dat 'algemeen aanvaard' is dat het voor mobiele aanbieders bij spam-, virus- en malwarebestrijding niet volstaat om alleen naar de headers van packets te kijken onvoldoende is onderbouwd.<sup>457</sup>

#### *Inlaten met bedrijfsvoering Vodafone*

Vodafone merkt in haar zienswijze 2 op dat het CBP zich op detailniveau inlaat met de dagelijkse bedrijfsvoering van Vodafone door niet of nauwelijks gemotiveerde voorstellen<sup>458</sup> hoe Vodafone haar technische bedrijfsvoering zou moeten inrichten (terwijl het CBP niet in overleg wil treden met Vodafone daarover). Dat is volgens Vodafone onzorgvuldig, het CBP treedt daarmee buiten zijn bevoegdheden én het is in strijd met de vrijheid van ondernemerschap (artikel 16 van het Handvest van de grondrechten van de Europese Unie (Handvest)).<sup>459</sup>

#### *Niet-neutrale toon<sup>460</sup> en vooringenomenheid*

Vodafone stelt zich op het standpunt dat het CBP blijft vasthouden aan suggestieve indelingen en beschrijvingen die niet stroken met de werkelijkheid. Vodafone verwijst in dat verband naar de volgende aspecten/elementen:

---

<sup>453</sup> Idem, p. 4-5 en 51-52, 54, 63 en 71.

<sup>454</sup> Zie idem, p. 5-6 en 59.

<sup>455</sup> Idem, p. 21 en 56.

<sup>456</sup> Idem, p. 5-6.

<sup>457</sup> Idem, p. 37.

<sup>458</sup> Zie ook idem, p. 55.

<sup>459</sup> Idem, p. 6-7, 55, 65, 68 en 70.

<sup>460</sup> Vgl. ook idem, p. 22.

- (i) de termen 'packet inspection', 'data-analyse technieken', 'gegevens over en uit het mobiele dataverkeer' - waarbij 'gegevens uit het dataverkeer' suggereert dat Vodafone de inhoud van communicatie van haar eindgebruikers kan inzien of zelfs inziet (wat onjuist is, behoudens de gevallen waarin dat ook volgens het CBP niet anders kan)<sup>461</sup>, 'gevoelige gegevens', 'persoonsgegevens die ook communicatie betreffen dan wel verkeersgegevens zijn', 'content type' en 'inspecteren' (in plaats van het door Vodafone voorgestelde 'beschikbaar' zijn van deze informatie)<sup>462</sup>: (alle) geen vastomlijnde en in de praktijk gangbare begrippen;<sup>463</sup>
- (ii) de metafoor van de brief en de envelop;<sup>464</sup>
- (iii) [VERTROUWELIJK];<sup>465</sup>
- (iv) dat 'het gebruik van data-analyse technieken veel mensen raakt', in combinatie met een verwijzing naar 21,8 miljoen mobiele aansluitingen;<sup>466</sup>
- (v) [VERTROUWELIJK];<sup>467</sup>
- (vi) Vodafone betwist de juistheid van de kwalificatie van de headergegevens in lagen 2 tot en met 7 van het OSI-model als gegevens 'over' het dataverkeer en meent dat het CBP het OSI- en TCP-IP-model nog steeds te weinig objectief gebruikt. Dit omdat inhoud van het verkeer/payload in dit Conceptrapport definitieve bevindingen is gedefinieerd als gegevens 'uit' het dataverkeer, terwijl zowel hostname/URL en IP-adres nodig zijn om het transport van data mogelijk te maken;<sup>468</sup>
- (vii) de passage in Hoofdstuk 1 van het Conceptrapport definitieve bevindingen over herkenning/identificatie van Skype-verkeer moet volgens Vodafone worden verwijderd. Dit omdat het CBP handhaving van de 'Zorgeloos Internet Blox' buiten de reikwijdte van het onderzoek laat en dit voorbeeld - in verband met het feit dat Vodafone vanaf 1 januari 2013 uitsluitend netneutrale proposities zal aanbieden - niet langer illustratief en kenmerkend is voor de wijze waarop door Vodafone op andere plekken data-analyse technieken worden ingezet. Vodafone heeft dat weliswaar eerder deep packet inspection genoemd, maar zonder daar de betekenis aan te willen geven die het CBP daar nu aan koppelt;<sup>469</sup>
- (viii) het CBP hanteert niet consequent de omschrijving van 'verkeersbeheer' uit de tabel met het overzicht doeleinden uit Hoofdstuk 2 van het Conceptrapport definitieve bevindingen, waarbij het doeleinde 'netwerkmonitoring' - in het bijzonder het oplossen en voorkomen van storingen en andere vormen van kwaliteitsmanagement van het netwerk' - een aparte categorie, al dan niet binnen 'verkeersbeheer', dient te zijn;<sup>470</sup>
- (ix) Vodafone weerspreekt het belang en de mogelijkheden van de door het CBP aangehaalde initiatieven en activiteiten om netwerkaanbieders te

<sup>461</sup> Zie idem, p. 7, 11-12 en 22 en 25.

<sup>462</sup> Idem, p. 31.

<sup>463</sup> Zie idem, p. 11.

<sup>464</sup> Idem, p. 7 en 25.

<sup>465</sup> Zie idem, p. 7 en 59-61.

<sup>466</sup> Idem, p. 12.

<sup>467</sup> Idem, p. 22-23.

<sup>468</sup> Idem, p. 23.

<sup>469</sup> Idem, p. 24.

<sup>470</sup> Idem, p. 25-26.

- helpen om te gaan met het grotere aantal signaleringen als gevolg van smartphones en apps (mede gelet op het tijdsverloop);<sup>471</sup>
- (x) de term ‘minder nadelige wijze’ waar het gaat om lichtere maatregelen.<sup>472</sup>

Dit bezien in combinatie met het feit dat het CBP niet in overleg wil treden met Vodafone en de in de ogen van Vodafone voor het CBP voordelige interpretatie van de wettelijke regels wijst volgens Vodafone op strijd met het verbod van vooringenomenheid (artikel 2:4 van de Awb). Daarbij is ook van belang, aldus Vodafone, dat de aanleiding van het onderzoek door OPTA en (later) het CBP (en de politiek-bestuurlijke bemoeienis) zich inmiddels heeft vertaald in (netneutraliteits-) wetgeving (artikel 11.2a en 7.4a van de Tw), waaraan Vodafone zich zal houden.<sup>473</sup>

#### *Communicatierealiteit anno 2012*

Volgens Vodafone heeft het CBP weinig oog voor de communicatierealiteit anno 2012, waarbij maatschappelijke (contractuele) belangen van eindgebruikers en bijbehorende (maatschappelijke) verplichtingen van Vodafone, zoals ten aanzien van kwaliteit en continuïteit van de dienstverlening (ook bijvoorbeeld ten aanzien van de monitoring van patiënten in ziekenhuizen, aansturing van trams of de bewaking van veroordeelden die via een enkelband bij hun huisarrest bewaakt worden<sup>474</sup>), zwaarwegende belangen zijn. Dit naast de belangen van de eindgebruiker omtrent het (wettige en zorgvuldige) gebruik van zijn persoonsgegevens. Vodafone stelt zich op het standpunt dat het CBP in de belangenafweging die het moet maken zich (ten onrechte) eenzijdig richt op de vermeende, vooral theoretische impact op de privacy van de eindgebruiker.<sup>475</sup>

#### *Opzet en structuur rapport*

Vodafone geeft in haar zienswijze 2 aan dat het Conceptrapport definitieve bevindingen volgens haar inconsistent is van opzet en structuur, waarbij feiten, juridisch kader (op fragmentarische wijze<sup>476</sup>) en beoordeling door elkaar lopen.<sup>477</sup> Zo merkt Vodafone bijvoorbeeld op dat in Hoofdstuk 1 (Inleiding) al een deel van het wettelijke kader wordt uiteengezet, Hoofdstuk 2 (Feitelijke bevindingen) tal van juridische kwalificaties bevat, in Hoofdstuk 3 (Uitwerking van het wettelijk kader en beoordeling) het wettelijk kader en de beoordeling (ten onrechte) gezamenlijk (in plaats van in separate hoofdstukken) en in een voor het CBP voordelige interpretatie worden gepresenteerd en per hoofdstuk steeds onderdelen van de zienswijze 1 van Vodafone van een reactie worden voorzien in een soort repliek-dupliekachtige stijl (in plaats van in een separate bijlage).<sup>478</sup>

#### **Geen criminal charge**

**Reactie CBP:** Vodafone beroept zich in haar zienswijze 2, onder verwijzing naar artikel 6 van het EVRM, op de onschuldpresumptie en het uitgangspunt dat een

---

<sup>471</sup> Idem, p. 30.

<sup>472</sup> Idem, p. 62.

<sup>473</sup> Idem, p. 7.

<sup>474</sup> Zie idem, p. 26.

<sup>475</sup> Idem, p. 8 en 65.

<sup>476</sup> Idem, p. 14.

<sup>477</sup> Zie ook idem, p. 22 en 40-41. Vgl. ook idem, p. 52.

<sup>478</sup> Idem, p. 8-9, 14 en 24-25.

verdachte niet hoeft mee te werken aan zijn eigen veroordeling (het nemo tenetur-beginsel).

In de toezichtfase kan de betrokkene nog geen beroep doen op dit beginsel. Het nemo tenetur-beginsel geldt vanaf het moment dat sprake is van een criminal charge.<sup>479</sup> Veelal wordt aangenomen dat sprake is van een criminal charge vanaf het tijdstip waarop de overtreder uit handelingen van het bestuursorgaan redelijkerwijs kan afleiden dat hem een boete zal worden opgelegd/dat naar objectieve maatstaven door een redelijk waarnemer kan worden vastgesteld dat sprake is van een 'verhoor' met het oog op de oplegging van een bestuurlijke boete (zie artikel 5:10a van de Awb).<sup>480</sup> Vanaf dat tijdstip is hij niet meer verplicht ten behoeve van de boeteoplegging enige verklaring over de overtreding af te leggen.<sup>481</sup>

In dit onderzoek (toezichtsfase) gaat het niet om een situatie waarin het bestuursorgaan overweegt om de overtreding 'punitief' af te doen, althans niet (langer) overweegt om (alleen) een herstelsanctie op te leggen. Om die reden is van een criminal charge in dit geval geen sprake. Vodafone heeft uit handelingen van het CBP in redelijkheid ook niet de verwachting kunnen ontleenen dat haar ter zake van de geconstateerde overtreding van de meldingsplicht een boete zal worden opgelegd. Er is Vodafone, zoals zij terecht opmerkt, geen cautie gegeven, in de aanbiedingsbrieven bij het Rapport voorlopige bevindingen en het Conceptrapport definitieve bevindingen is enkel opgemerkt *"Het CBP heeft de bevoegdheid om bestuursrechtelijke maatregelen te treffen zoals het opleggen van een last onder dwangsom bij voortdurende van een geconstateerde onrechtmatigheid"* en het CBP heeft sinds 2007 geen boetes opgelegd ter zake van overtreding van de meldingsplicht<sup>482</sup> (wel is de meldingsplicht in de laatste jaren opgetreden met een herstelsanctie<sup>483</sup>).

Anders dan Vodafone heeft betoogd, maakt de omstandigheid dat de geconstateerde overtreding van de meldingsplicht kan worden gesanctioneerd met een bestuurlijke boete (ook) niet dat de waarborgen van artikel 6 van het EVRM zich uitstrekken over het gehele onderzoek. Alleen al omdat geen sprake is van een criminal charge kan

---

<sup>479</sup> Zie o.a. EHRM 25 februari 1993, NJ 1993/485 (Funke) en AbRvS 19 september 1996, AB 1997, 91.

<sup>480</sup> Zie o.a. HR 17 februari 1987, NJ 1987/951; EHRM 27 februari 1980, NJ 1980/561 (Deweert); *Kamerstukken II* 2005/06, 29 702, nr. 7, p. 41 en *T&C Algemene wet bestuursrecht*, commentaar op artikel 5:10a Awb.

<sup>481</sup> Zie o.a. EHRM 17 december 1996, NJ 1997/699 (Saunders) en CRvB 21 november 2012, AB 2013, 27.

<sup>482</sup> URL: [http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2012.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2012.pdf);  
[http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2011.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2011.pdf);  
[http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2010.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2010.pdf);  
[http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2009.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2009.pdf);  
[http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2008.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2008.pdf) en  
[http://www.cbpweb.nl/downloads\\_jaarverslagen/jv\\_2007.pdf](http://www.cbpweb.nl/downloads_jaarverslagen/jv_2007.pdf). Zie ook  
[http://cbpweb.nl/downloads\\_pb/pb\\_20091218\\_advance\\_bevindingen.pdf](http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf) en  
[http://www.cbpweb.nl/Pages/einde\\_vervolgprocedure\\_advance.aspx](http://www.cbpweb.nl/Pages/einde_vervolgprocedure_advance.aspx) (URL's laatst bezocht op 29 mei 2013).

<sup>483</sup> URL:  
[http://www.cbpweb.nl/Pages/pb\\_20110811\\_google.aspx](http://www.cbpweb.nl/Pages/pb_20110811_google.aspx) en  
[http://www.cbpweb.nl/downloads\\_pb/pb\\_20110419\\_brief\\_google\\_lod.pdf](http://www.cbpweb.nl/downloads_pb/pb_20110419_brief_google_lod.pdf) (URL's laatst bezocht op 29 mei 2013).



derhalve ook geen sprake zijn van een zodanige nauwe verwevenheid, zowel juridisch als feitelijk, van een niet-punitieve bestuursrechtelijke procedure en een punitieve procedure (bestuurlijke boete) dat het gehele onderzoek dient te worden beoordeeld in het kader van artikel 6 van het EVRM.<sup>484</sup>

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

### **Geen fishing expedition**

Vodafone meent dat zij door onduidelijkheid omtrent de reikwijdte en het onderwerp van onderzoek en de onderzoeksvragen is gedwongen om mee te werken aan haar eigen veroordeling.

Een fishing expedition waarbij via dwang ongericht informatie wordt verzameld, is in het kader een punitieve procedure in het licht van het EVRM niet toegestaan.<sup>485</sup> Zoals hierboven gemotiveerd onder het kopje ‘Geen criminal charge’, is van een criminal charge in dit onderzoek geen sprake. Evenmin is door de toezichthouders van het CBP buitensporig gezocht naar bewijs, zonder dat doel en voorwerp van het onderzoek nauwkeurig waren omschreven.

Er was een redelijke aanleiding zijn om op onderzoek uit te gaan. OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van artikel 10, eerste en derde lid, van het Samenwerkingsprotocol CBP-OPTA jo. artikel 24, tweede lid, van de Wet OPTA. In haar voorlopige bevindingen heeft OPTA hierover opgemerkt: *“Het is voor het college [van de OPTA, toevoeging door het CBP] nog niet duidelijk of de inzet van de door de aanbieders gebruikte analysemiddelen en de daarbij verwerkte gegevens in alle gevallen gerechtvaardigd en proportioneel is in het licht van de zorgplicht van artikel 11.2 Tw. (...) Daarvoor is nader onderzoek nodig. Het is daarbij van belang dat artikel 11.2 Tw nauw samenhangt met het bepaalde in de Wet bescherming persoonsgegevens, waarop het CBP toeziet. Het CBP en het college hebben hierover overlegd. Op grond van het samenwerkingsprotocol is besloten dat het college zijn bevindingen en de onderzoeksgegevens naar de naleving van artikel 11.2 van de Tw ter beschikking stelt aan het CBP. Het CBP zal deze bevindingen en de onderzoeksgegevens betrekken bij zijn onderzoek naar de naleving van de Wbp en de verwerking van persoonsgegevens bij de inzet van DPI-technieken.”*<sup>486</sup>

In zijn aankondiging van het onderzoek heeft het CBP als reikwijdte en onderwerp van het onderzoek genoemd dat het *“een ambtshalve onderzoek [heeft, toevoeging door het CBP] ingesteld naar de wijze waarop bij het gebruik van packet inspection technologie en technieken [voetnoot CBP: Onder packet inspection technologie en technieken wordt in elk geval, maar niet uitsluitend, verstaan Shallow en Deep Packet Inspection] door*

---

<sup>484</sup> Vgl. EHRM 5 april 2012, AB 2012, 323. Zie ook Rb. Arnhem 21 februari 2013, LJN BZ1604, BZ1617 en BZ1707.

<sup>485</sup> Zie o.a. EHRM 3 mei 2001, AB 2002, 343 (J.B. vs Zwitserland) en EHRM 21 april 2009, NJ 2009, 557 (Marttinen).

<sup>486</sup> ‘Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken’, *Onderzoek OPTA* 30 juni 2011. URL: <https://www.acm.nl/nl/publicaties/publicatie/10234/Voorlopige-bevindingen-over-gebruik-Deep-Packet-Inspection/> (URL laatst bezocht op 29 mei 2013).

*Vodafone Libertel B.V. (Vodafone) toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp.*"

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

Het CBP heeft geen andere bescheiden of zaken (nader) onderzocht dan die welke verband houden met de wettelijke voorschriften waarop het toezicht in dit onderzoek betrekking heeft. Voor zover het CBP (aanvullende) inlichtingen en inzage in zakelijke gegevens en bescheiden heeft gevorderd, merkt Vodafone in haar reactie op dat de informatie moet worden gezien als *vrijwillig verstrekt* ontlastend bewijs.<sup>487</sup> Ook de omstandigheid dat de inzet van data-analyse technieken voor de facturering van MMS-verkeer en het filteren op inkomende spam naar aanleiding van de zienswijze 1 respectievelijk zienswijze 2 van Vodafone (alsnog) buiten de scope van dit onderzoek is verklaard, maakt niet dat het onderzoek onzorgvuldig is (geweest) en om die reden moet worden beëindigd. Vodafone is daardoor ook niet in haar belangen geschaad.

De zienswijze 2 van Vodafone heeft op het punt van het niet beoordelen van de gegevensverwerking die verband houdt met de Dienstvoorwaarden Vodafone BloX vanwege de beëindiging/uitfasering daarvan (wel) geleid tot aanpassing en verduidelijking van het rapport (consistentie van de tekst op dit punt). De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

### **Hoor en wederhoor**

Voor zover Vodafone zich op het standpunt stelt dat het CBP niet (eerst) een Conceptrapport definitieve bevindingen aan haar had mogen voorleggen voor een tweede zienswijze, wijst het CBP erop dat het niet onzorgvuldig is om een partij opnieuw gelegenheid te bieden tot het geven van zienswijzen. In uitzonderlijke gevallen zal een bestuursorgaan op grond van de algemene beginselen van behoorlijk bestuur zelfs verplicht zijn om indieners van zienswijzen in de gelegenheid te stellen een nieuwe zienswijze naar voren te brengen in verband met voorgenomen wijzigingen naar aanleiding van ingebrachte zienswijzen.<sup>488</sup> Vodafone heeft in haar zienswijze 1 overigens zelf aangegeven: *"Ook als het Rapport zou worden gewijzigd, dient Vodafone nadere gelegenheid te krijgen om het aangepaste Rapport te beoordelen (...)".*<sup>489</sup>

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

<sup>487</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 11.

<sup>488</sup> CBb 3 november 2009, AB 2009, 402.

<sup>489</sup> Zienswijze 1 Vodafone, p. 6 (doorgenummerde pagina's op de faxbrief).

### **Reformatio in peius**

Vodafone betoogt in haar zienswijze 2 dat in het Conceptrapport definitieve bevindingen sprake is van een verboden 'reformatio in peius', nu het CBP een extra overtreding constateert doordat Vodafone voor het doeleinde behandeling van verzoeken om inlichtingen van klanten al gegevens verzamelt vóórdat een klant belt met een vraag of klacht, en ten aanzien van de informatieplicht.

Het verbod van reformatio in peius houdt in dat het instellen van bezwaar of beroep er niet toe mag leiden dat de indiener van het bezwaar- of beroepschrift in een slechtere positie komt dan zonder het instellen van bezwaar of beroep het geval zou zijn geweest (artikel 7:11 en 8:69 van de Awb). Er is geen wettelijk voorschrift of algemeen rechtsbeginsel dat meebrengt dat een indiener van een zienswijze niet in een nadeliger positie mag komen te verkeren als gevolg van zijn zienswijze.<sup>490</sup>

Doordat het CBP Vodafone in de gelegenheid heeft gesteld een nieuwe zienswijze naar voren te brengen is zij niet in haar verweermogelijkheden geschaad. Nog afgezien daarvan geldt dat de zienswijze 2 van Vodafone op het punt van de grondslag voor het doeleinde behandeling van verzoeken om inlichtingen van klanten (wel) heeft geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies dat het CBP ten aanzien van deze gegevensverwerking geen overtreding heeft geconstateerd van de wet. De zienswijze 2 van Vodafone heeft op het punt van de 'reformatio in peius' niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

### **Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering**

Vodafone doet in haar zienswijze 2 een beroep op de onschuldpresumptie (artikel 6 van het EVRM). Vodafone brengt verder naar voren dat het onderzoek c.q. Conceptrapport van bevindingen (kort gezegd) onzorgvuldig is voorbereid en ontoereikend is gemotiveerd. Zo motiveert het CBP volgens Vodafone onvoldoende waarom er ten aanzien van bepaalde data-analyse technieken (te weten: de (sub)doeleinden verkeersbeheer en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardesites) alternatieve, voor de betrokken eindgebruikers vermeend lichtere (dat wil zeggen: minder ingrijpende) maatregelen kunnen worden gebruikt (ten onrechte is ook niet in kaart gebracht wat de gevolgen, bijvoorbeeld voor de netwerkintegriteit en stabiliteit, zouden zijn van zulke alternatieven). Ook verwijt Vodafone het CBP weinig oog te hebben voor maatschappelijke (contractuele) belangen van eindgebruikers en bijbehorende (maatschappelijke) verplichtingen van Vodafone, zoals ten aanzien van kwaliteit en continuïteit van de dienstverlening.

Zoals hierboven gemotiveerd onder het kopje 'Geen criminal charge', is van een criminal charge in dit onderzoek geen sprake. Er geldt daarom geen 'onschuldpresumptie'.

Ten aanzien van de 'reguliere' onderzoeksplicht in artikel 3:2 van de Awb geldt dat hoofdregel is dat bij het nemen van een belastende beschikking de bewijs(voerings)last in beginsel op het bestuursorgaan rust. Niettemin kan zich de

---

<sup>490</sup> Vgl. ook AbRvS 14 maart 2012, L/JN BV8812.

situatie voordoen dat bijvoorbeeld uit de parlementaire geschiedenis van een wetsartikel blijkt welke partij de bewijslast zou moeten dragen.<sup>491</sup> De plicht om de noodzaak van de verwerking aan te tonen berust onder het Wbp-regime bij de verantwoordelijke.<sup>492</sup> Zie voor een nadere toelichting van het toepasselijke en toegepaste wettelijk kader 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, het kopje 'Samenloop Wbp en Tw'. Ook de volgende factoren (vuistregels) kunnen de verdeling van de bewijslast beïnvloeden: de partij die belang heeft bij een bepaald feit, draagt de bewijslast, de partij in wier bewijsdomein het feit ligt, draagt de bewijslast en de partij die zich op een uitzondering of een verandering beroept, draagt de bewijslast.<sup>493</sup> Zo bevat artikel 11.5 van de Tw een verwijderings-/anonimiseringsplicht en beroept Vodafone zich op (een) uitzondering(en) daarop.

Om aan de bewijs(voerings)last te voldoen, zal het bestuursorgaan onderzoek instellen naar de feiten. Het bestuursorgaan dient bij de voorbereiding van onder andere een besluit de nodige kennis te vergaren omtrent de relevante feiten en de af te wegen belangen (artikel 3:2 jo. 3:1 van de Awb). Bij ingrijpendere besluiten worden in het algemeen zwaardere eisen aan het onderzoek gesteld. Neemt het bestuursorgaan een feitelijke stelling in, dan moet het deze stelling (vervolgens) met concrete feiten onderbouwen (geen schatting, subjectieve overtuiging of prognose, wel een voldoende concreet en sterk vermoeden).<sup>494</sup> Heeft het bestuursorgaan de rechtsfeiten aannemelijk gemaakt - wordt vermoed dat de rechtsfeiten zich hebben voorgedaan, dan is het aan de belanghebbende om de onjuistheid van de vergaarde gegevens aannemelijk te maken.<sup>495</sup> Er mogen niet dermate zware eisen aan het vermoeden worden gesteld, dat de uitvoering van de bestuursbevoegdheid teveel wordt gefrustreerd.<sup>496</sup>

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

Heeft een besluit negatieve consequenties dan zal het bestuursorgaan die nadelige consequenties moeten inventariseren. Op het bestuursorgaan rust ter zake een onderzoeksplicht. Voldoende is als het bestuursorgaan de betrokken belangen

---

<sup>491</sup> Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 111.

<sup>492</sup> *Kamerstukken II 1998/99, 25 892, nr. 13, p. 6*: "Overigens wijzen wij erop dat alleen een gerechtvaardigd belang niet voldoende is. Gegevensverwerking is blijkens artikel 8, onder f, alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook «noodzakelijk» is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke."

<sup>493</sup> Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 137-141.

<sup>494</sup> *Idem*, p. 91 en 104. Zie ook CBb 7 juli 2004, LJN AQ1048: "Verweerder mag zijn oordeel dienaangaande mede baseren op vermoedens, mits deze vermoedens voldoende concreet en sterk zijn."

<sup>495</sup> Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 103-104.

<sup>496</sup> *Idem*, p. 105. Zie ook CBb 29 april 2004, AB 2004, 317.

inventariseert en bij de belanghebbende navraagt in welke mate haar belang door het voorgenomen besluit wordt geschaad. Het is aan de belanghebbende om aan de hand van bijzondere feiten en omstandigheden de schending van het evenredigheidsbeginsel aannemelijk te maken. De belanghebbende draagt de bewijslast voor de stelling dat zijn belang door het besluit onevenredig zwaar wordt getroffen.<sup>497</sup> Wel blijft het bestuursorgaan verantwoordelijk voor een deugdelijke belangenafweging.

Ten aanzien van de motiveringsplicht geldt dat de motivering het besluit moet kunnen dragen (artikel 3:46 jo. 3:1 van de Awb): een juiste vaststelling van de feiten die mag leiden tot het genomen besluit.<sup>498</sup>

Het CBP heeft zorgvuldig feitenonderzoek verricht.<sup>499</sup> Het CBP heeft Vodafone bezocht en op verschillende moment gedurende het onderzoek inlichtingen en inzage in zakelijke gegevens en bescheiden gevraagd en vergaard van Vodafone omtrent de wijze waarop de gegevensverwerking plaatsvindt, te weten: de categorieën van (soorten) gegevens, de verwerkingshandelingen, de duur van de verwerking, en daarmee samenhangend de configuratie-instellingen van de ingezette data-analyse apparatuur, alsmede voor welke doeleinden (zie het kopje 'Verloop onderzoek' voor een beschrijving van de ingezette toezichtshandelingen, waaronder het bekijken van (gebruikers)interfaces van de apparatuur die Vodafone inzet voor data-analyse, p. 10 e.v. van dit rapport).

Het rapport bevat (daarnaast) een weerslag van verzamelde kennis op basis van de aanwezigheid van de vereiste expertise bij het bestuursorgaan zelf over mogelijkheden tot het niet langer beschikbaar houden (verwijderen) van gegevens met persoonsidentificerende kenmerken dan noodzakelijk is en het anonimiseren van persoonsgegevens. Gelet op deze kennis, in samenhang gezien met een analyse van de door Vodafone beschikbaar gestelde inlichtingen en zakelijke gegevens en bescheiden omtrent de wijze waarop de gegevensverwerking plaatsvindt en voor welke doeleinden, heeft het CBP (daarna) gesteld dat er ten aanzien van bepaalde data-analyse technieken (in het kader van de 'subdoeleinden' netwerkplanning, netwerkmonitoring en het transporteren van het verkeer van prepaidklanten naar

---

<sup>497</sup> Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 120. Zie o.a. AbRvS 15 oktober 1998, JB 1998, 278 en ABRS 18 september 2002, AB 2003, 132: "(...) Dit neemt niet weg dat zich feiten en/of omstandigheden kunnen voordoen waardoor een individueel belang ten gevolge van een dergelijke maatregel zodanig zwaar wordt getroffen dat het bestuursorgaan, na afweging van de betrokken belangen, niet in redelijkheid tot het treffen van de verkeersmaatregel heeft kunnen besluiten, dan wel het nadeel daarvan redelijkerwijs niet ten laste van betrokkene dient te blijven. Dat sprake is van dergelijke feiten en omstandigheden dient in beginsel door betrokkene aannemelijk te worden gemaakt."

<sup>498</sup> T&C Algemene wet bestuursrecht, commentaar op artikel 3:46 Awb.

<sup>499</sup> Zie over de zorgvuldigheid van het onderzoek AbRvS 15 augustus 2012, LJN BX4694: "Anders dan De Koers ter zitting heeft betoogd, is er geen grond voor het oordeel dat de inspectie geen zorgvuldig feitenonderzoek heeft verricht. De inspectie heeft ter uitvoering van de tussenuitspraak De Koers op 30 september 2011 bezocht en gesprekken gevoerd met de directie, leerlingen, leraren, begeleiders en het bevoegd gezag. De inspectie heeft onderzocht welke leerbronnen de school inzet, heeft leerlingenvoer en leerlingendossiers bekeken en de door De Koers beschikbaar gestelde documenten geanalyseerd. Gezien deze onderzoeksactiviteiten is er geen reden voor het oordeel dat dit onderzoek onzorgvuldig is."

(gratis) opwaardeersites) alternatieve maatregelen kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is (als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren). Vervolgens heeft het CBP op conceptueel niveau en in het Rapport voorlopige bevindingen ook met een concreet voorbeeld, onderbouwd hoe de informatiesystemen zouden kunnen worden vormgegeven, zonder (te) vergaand in te willen grijpen in de bedrijfsprocessen en bedrijfsvoering van Vodafone. Gedacht kan worden aan bijvoorbeeld voor verkeersbeheer het toevoegen van een zogeheten privacy filter om gegevens met persoonsidentificerende kenmerken onmiddellijk na het verzamelen te verwijderen of onomkeerbaar te anonimiseren en voor het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed aan het verlenen van toegang tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een opwaardeer-/betalingswebsite kan bezoeken. Van belang is daarbij waar het gaat om de haalbaarheid van zulke alternatieven dat het uitgangspunt van de Europese wetgever is geweest ten aanzien van het ontwikkelen van informatiesystemen voor de telecommunicatiemarkt dat deze *“systemen voor elektronische-communicatienetwerken en -diensten (...) op dusdanige wijze [moeten, toevoeging door het CBP] worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. Activiteiten die betrekking hebben op het aanbieden van elektronische-communicatiediensten en verder gaan dan de transmissie van communicatie en de facturering ervan moeten gebaseerd worden op geaggregeerde verkeersgegevens die niet met abonnees of gebruikers in verband kunnen worden gebracht (...)”*, (overweging 30 van de e-Privacyrichtlijn).

Het CBP heeft Vodafone tweemaal in de gelegenheid gesteld om op het bewijsmateriaal te reageren/tegenbewijs te leveren. Vodafone heeft om de onjuistheid van de vergaarde gegevens aannemelijk te maken het volgende ingebracht. In haar zienswijze 1 heeft Vodafone tegenbewijs geleverd door overlegging van een verklaring van één van haar leveranciers ([VERTROUWELIJK]) dat het concrete voorbeeld van het CBP geen lichtere maatregel is (maar wel een significante verslechtering van de dienstverlening zal betekenen).<sup>500</sup> Gelet daarop is dit concrete voorbeeld niet gehandhaafd in het Conceptrapport definitieve bevindingen. In aanvulling daarop heeft Vodafone in haar zienswijze 2 (onder andere) betwist dat de [VERTROUWELIJK: apparatuur] en [VERTROUWELIJK: apparatuur] die zij inzet voor verkeersbeheer gegevens eerder kan anonimiseren, zonder bijvoorbeeld een geheel nieuw product te (laten) ontwikkelen.<sup>501</sup> Ten aanzien van de [VERTROUWELIJK: apparatuur] heeft zij daar in haar reactie op de vordering van het CBP aan toegevoegd: *“(...) Het zou, doch slechts in theorie - immers: de categorieën zijn niet los van elkaar te zien (...), wel mogelijk om op het niveau van de [VERTROUWELIJK: apparatuur] categorieën gegevens er uit te filteren”; hiermee wordt echter niet afgedaan aan het feit dat analyse (op centraal netwerkniveau) reeds heeft plaatsgevonden.”*<sup>502</sup> Het CBP mag hieruit afleiden dat enkel aanpassing van de configuratie-instellingen in het geval van de [VERTROUWELIJK: apparatuur] en [VERTROUWELIJK: apparatuur] geen alternatief is. Vodafone heeft met haar zienswijzen op dit punt echter géén gerede

<sup>500</sup> Zienswijze 2 Vodafone, p. 9, 57 en 65. Zienswijze 1 Vodafone, p. 22 (doorgenummerde pagina's op de faxbrief) en bijlage 2 bij deze zienswijze.

<sup>501</sup> Zie o.a. Zienswijze 2 Vodafone, p. 9-10, 55-57 en 65. Reactie Vodafone op vordering van 21 februari 2013, p. 9. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 10.

<sup>502</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 9. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 9.

twijfel opgewekt over de juistheid van de feitelijke stelling van het CBP dat er in algemene zin alternatieve maatregelen zijn die kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is. [VERTROUWELIJK] Zie hierover verder de zienswijzebeantwoording onder het kopje ‘Geen andere, minder ingrijpende middelen om het zelfde resultaat te bereiken’).

Het CBP heeft de nadelige consequenties voor Vodafone en (eventueel) haar klanten van het niet zo lang in niet-geanonimiseerde vorm mogen verwerken van de persoonsgegevens geïnventariseerd, bijvoorbeeld voor de netwerkindegriteit en stabiliteit, hoofdzakelijk beschreven in haar zienswijzen, en op een rij gezet in het rapport onder de kopjes ‘Technische alternatieven’ en ‘Prepaidverkeer’ in **bijlage IV** en het kopje ‘Geen andere, minder ingrijpende middelen om het zelfde resultaat te bereiken’ in deze **bijlage V** bij dit rapport. Naar aanleiding van de zienswijze 2 van Vodafone heeft het CBP door middel van zijn vordering aan Vodafone nagevraagd in welke mate zijn belang, bijvoorbeeld de netwerkindegriteit en stabiliteit, wordt geschaad als zij de persoonsgegevens niet zo lang in niet-geanonimiseerde vorm mag verwerken: *“of, in hoeverre en zo ja, op welke wijze andere factoren dan (de configuratie-instellingen op) de thans bij u in gebruik zijnde data-analyse apparatuur een rol spelen bij uw beantwoording van deze vraag naar de noodzaak om de gegevens over en/of uit het mobiele dataverkeer - ook na het verzamelen daarvan - in niet-geanonimiseerde vorm te verwerken, bijvoorbeeld congestierisico’s of andere kwetsbaarheden die specifiek zijn voor uw netwerk(-infrastructuur)”*. Tevens het CBP daarmee in kaart gebracht en bevat dit rapport een inschatting van de kosten (in euro's) en de tijd die het kost (in kalenderdagen) om voor het ‘subdoeleinde’ verkeersbeheer (een) data-analyse oplossing(e) te (laten) ontwikkelen, implementeren en beheren die Vodafone in staat zou stellen om de persoonsgegevens onmiddellijk na het verzamelen onomkeerbaar in niet-persistent (werk)geheugen te anonimiseren of zodanig te aggregeren dat deze niet met individuele klanten in verband kunnen worden gebracht dan wel om de verwerking van niet-geanonimiseerde gegevens te beperken tot die klanten die daarvoor hun (ondubbelzinnige) toestemming hebben gegeven.<sup>503</sup>

De zienswijze 2 van Vodafone heeft op het punt van de weergave van de zienswijze 1 van Vodafone in de inleiding in het rapport geleid tot aanpassing, te weten: aanvulling en verduidelijking van de samenvatting van zienswijze 1. De zienswijze 2 van Vodafone heeft op het punt van de plicht tot zorgvuldige kennisvergaring en een zorgvuldige belangenafweging geleid tot aanvulling en verduidelijking van de geïnventariseerde en meegewogen belangen in dit rapport. De zienswijze 2 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

### **Onderzoek in tijd en omvang begrensd**

Vodafone stelt zich in haar zienswijze 2 op het standpunt dat nu de toezichthouder de juiste feiten niet boven tafel heeft weten te krijgen in een onderzoek in tijd, omvang en gelegenheden begrensd de rechtszekerheid en artikel 6 van het EVRM (afdoening binnen een redelijke termijn) vereisen dat het onderzoek moet worden gesloten.

Voor de vraag wanneer kan worden gesproken van een overschrijding van de redelijke termijn geldt als vertrekpunt bij niet-punitieve procedures het moment

---

<sup>503</sup> Vordering CBP inlichtingen en inzage in zakelijke gegevens en bescheiden van 20 december 2012 en herstellvordering CBP van 7 maart 2013.

waarop sprake is van een geschil. Dat is doorgaans het moment waarop een bezwaarschrift wordt ingediend tegen het (uitblijven van een) besluit. In die situaties waarin sprake is van een uniforme openbare voorbereidingsprocedure (afdeling 3.4 van de Awb) lijkt van een geschil te kunnen worden gesproken op het moment dat een zienswijze wordt ingediend tegen het ontwerpbesluit.<sup>504</sup> Als vertrekpunt bij punitieve procedures geldt dat de termijn begint te lopen op het moment dat de overtreder duidelijk is dat een hem een boete zal worden opgelegd. Dat lijkt het moment waarop toezending van de definitieve versie van het boeterapport heeft plaatsgevonden.<sup>505</sup>

Zoals hierboven gemotiveerd onder het kopje ‘Geen criminal charge’, is van een criminal charge in dit onderzoek geen sprake. Voor zover Vodafone bedoelt te stellen dat de eisen van artikel 6 van het EVRM door middel van het rechtszekerheidsbeginsel een rol spelen, geldt dat er (nog) geen besluit ligt. De termijn is in dit onderzoek daarom nog niet aangevangen.

Daar komt bij dat alleen vertragingen die moeten worden toegerekend aan het bestuursorgaan bepalend kunnen zijn voor de motivering van het oordeel dat de redelijke termijn is overschreden. Bij het vergaren van de nodige kennis omtrent de relevante feiten en de af te wegen belangen stuitte het CBP op afwijkend, (schijnbaar) inconsistent (bewijs)materiaal, zodat het nader onderzoek moest verrichten. Bijvoorbeeld waar het ging om de categorieën van (soorten) van verwerkte gegevens (IP-adressen, zendmastgegevens, [VERTROUWELIJK]), het anonimiseren en aggregeren daarvan en de bewaartermijn.

Het gaat hier verder om een omvangrijk onderzoek (parallel uitgevoerd met onderzoeken naar de andere drie grootste mobiele netwerkaanbieders in Nederland) in een juridisch en technisch ingewikkelde zaak. Wat betreft de juridische complexiteit speelt bijvoorbeeld een rol: de (op stapel staande) wetswijzigingen op het gebied van netneutraliteit en vertrouwelijkheid van communicatie.

De zienswijze 2 van Vodafone heeft op het punt van de omvang en duur van het onderzoek niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

#### **Fair play- en lex certa-beginsel: geen overleg over beëindigen geconstateerde overtredingen**

Vodafone betoogt in haar zienswijze 2 dat het in strijd met het fair play-beginsel, onzorgvuldig en in strijd met het zelfincriminatieverbod is dat het CBP niet in overleg wil treden met haar over de melding, de privacyverklaring, het terugbrengen van bewaartermijnen en het herhaaldelijke aanbod van Vodafone om in gezamenlijk overleg te overzien hoe eventuele overtredingen zo snel en zo effectief mogelijk kunnen worden beëindigd.

---

<sup>504</sup> A. ten Veen & A. Collignon, *De redelijke termijn voor bestuursorgaan en rechter*, p. 322. URL: <http://www.stibbe.nl/upload/11bae790e012d284e0bbf03e5f.PDF> (URL laatst bezocht op 29 mei 2013).

<sup>505</sup> Vgl. Rb. Rotterdam 4 mei 2011, *LJN BQ3528* en CBb 25 maart 2011, *LJN BQ5977* (procedures over een criminal charge).



De ene helft van het fair play-beginsel is neergelegd in artikel 2:4 van de Awb (zie daarover verder het kopje '(Schijn) van vooringenomenheid'). De andere helft van het fair-play beginsel houdt in dat een bestuursorgaan de burger de mogelijkheid geven zijn procedurele kansen te benutten (niet mag door het overheidsoptreden de rechtsbescherming worden gefrustreerd).<sup>506</sup>

Uit het legaliteitsbeginsel volgt dat een voorschrift dat door bestuurlijke sancties wordt gehandhaafd, voldoende duidelijk, voorzienbaar en kenbaar moet zijn (artikel 5:4 van de Awb: het lex certa-beginsel).<sup>507</sup>

Voor zover Vodafone een beroep bedoelt te doen op het in artikel 5:4 van de Awb vervatte lex certa-beginsel, merkt het CBP op dat de meldingsplicht in artikel 27 jo. 28 en de informatieplicht in artikel 34 van de Wbp voldoen aan het bepaalbaarheidsgebod. Zo zijn bijvoorbeeld de te melden gegevens (waaronder het doel of de doeleinden van de verwerking en een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben) duidelijk en precies geformuleerd in artikel 28, eerste lid, van de Wbp. De vraag welke informatie Vodafone aan de betrokkenen moet verstrekken, kan worden beantwoord aan de hand van de tekst van de wet, de wetsgeschiedenis van artikel 34 van de Wbp<sup>508</sup>, de Wbp-naslag van het CBP<sup>509</sup>, de CBP Richtsnoeren publicatie van persoonsgegevens op internet<sup>510</sup>, met als bijlage een model privacyverklaring en opinies van de Artikel 29-werkgroep.<sup>511</sup>

Er is geen wettelijk voorschrift of algemeen rechtsbeginsel dat meebrengt dat een toezichthouder gehouden is om in overleg met een overtreder, samen te bezien hoe de overtreder geconstateerde overtredingen kan beëindigen.

---

<sup>506</sup> Module Algemeen Bestuursrecht, MAB 129. Zie o.a. No 9 november 2005, AB 2006, 31; No 27 mei 2009, AB 2009, 284: *"Dit impliceert dat een bestuursorgaan, na ontvangst van een verzoek of bezwaarschrift, hierop adequaat dient te reageren door alle benodigde informatie te verzamelen, de burger en eventuele andere betrokkenen uit te nodigen om hun standpunt toe te lichten, en vervolgens op basis van de aldus verkregen en overige reeds te zijner beschikking staande informatie een beslissing te nemen, waarin het na afweging van alle in het geding zijnde belangen gemotiveerd zijn reactie op het verzoek of bezwaarschrift kenbaar maakt."*

<sup>507</sup> T&C Algemene wet bestuursrecht, commentaar op artikel 5:4 Awb. Zie o.a. EHRM 25 mei 1993

(Kokkinakis/Griekenland), zaaknummer 14307/88 en AbRvS 3 mei 2006, AB 2006, 317.

<sup>508</sup> Zie o.a. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 149-157.

<sup>509</sup> URL: <http://www.cbweb.nl/wbpnaslag/5/Paginas/Wbp-hoofdstuk-5-informatieverstrekking-aan-de-betrokkene.aspx> (URL laatst bezocht op 29 mei 2013).

<sup>510</sup> CBP Richtsnoerenpublicatie van persoonsgegevens op internet van december 2007, p. 25-28. URL:

[http://www.cbweb.nl/downloads\\_rs/rs\\_20071211\\_persoonsgegevens\\_op\\_internet\\_definitief.pdf](http://www.cbweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf) (URL laatst bezocht op 29 mei 2013).

<sup>511</sup> WP29 203. Opinion 03/2013 on purpose limitation van 2 april 2013. WP29 100. Advies 10/2004 over meer geharmoniseerde bepalingen inzake informatieverstrekking van 25 november 2004, met bijlagen. URL:

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100\\_nl.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_nl.pdf). WP29 43. Recommendation on certain minimum requirements for collecting personal data online in the European Union, dated 17 mei 2001. URL:

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp43en.pdf> (URL's laatst bezocht op 29 mei 2013).

Van een professionele marktdeelnemer, zoals Vodafone, mag worden verlangd dat deze zich terdege laten informeren over de beperkingen waaraan haar gedragingen zijn onderworpen. Vodafone heeft ook professionele rechtsbijstand (vanaf het Conceptrapport definitieve bevindingen).

Vodafone is tweemaal in de gelegenheid gesteld tot het geven van zienswijzen. Ten aanzien van de melding en de privacyverklaring geldt dat het CBP in het Rapport voorlopige bevindingen en het Conceptrapport definitieve bevindingen heeft beoordeeld en gemotiveerd op welke punten de betreffende documenten én de door Vodafone voorgestelde concepten - als voorgenomen maatregelen - (nog) niet voldoen aan de wettelijke vereisten. Het CBP heeft het nieuwe Privacy Statement van Vodafone van augustus 2012 in dit Rapport definitieve bevindingen meegenomen.

Voor het overige heeft Vodafone het CBP geen (voorgenomen) maatregelen voorgelegd met het verzoek deze ex ante te toetsen/mee te nemen in het onderzoek naar de vraag of de geconstateerde overtredingen daarmee zijn/worden beëindigd.

Niet kan worden geconcludeerd dat Vodafone haar procedurele kansen niet heeft kunnen benutten.

Daar komt bij dat indien en voor zover het CBP in dit rapport zijn bevindingen handhaaft en concludeert dat sprake is van voortdurende van (een) geconstateerde onrechtmatighe(i)d(en), Vodafone eerst (nogmaals) in de gelegenheid wordt gesteld om te worden gehoord.

De zienswijze 2 van Vodafone heeft op het punt van het fair play- en lex certa-beginsel geleid tot verduidelijking van de punten waarop de (concept-)melding en de privacyverklaring van Vodafone (nog) niet voldoen aan de wettelijke vereisten. De zienswijze 2 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport. De zienswijze 2 van Vodafone heeft op het punt van het toetsingskader voor de verwerking van URL's wel geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport.

### **Toekomstige regelgeving**

In haar zienswijze 2 maakt Vodafone er bezwaar tegen dat het CBP kwalificaties geeft over de rechtmatigheid van het gebruik van 'data-analyse technieken' onder nieuwe 'toekomstige' regelgeving (artikel 7.4a en artikel 11.2a van de Tw (nieuw)).

Vodafone heeft in haar zienswijze 1 zelf verwezen naar en een beroep gedaan op (de gevolgen van de) 'aanstaande wijzigingen van de Tw, met name artikel 7.4a en 11.2a'.<sup>512</sup> Om die reden is het niet onzorgvuldig dat het CBP in het Conceptrapport definitieve bevindingen is ingegaan op (de gevolgen van) deze nieuwe regelgeving. Deze wetsartikelen zijn inmiddels geldend recht, zodat (ook) om die reden in dit rapport moet worden getoetst aan deze artikelen.

---

<sup>512</sup> Zienswijze 1 Vodafone, p. 31-32 (doorgenummerde pagina's op de faxbrief).

De zienswijze 2 van Vodafone heeft op het punt van de verklaring van Vodafone dat zij alle huidige proposities die niet stroken met artikel 7.4a en 11.2a van de Tw vóór de inwerkingtreding van de relevante regels zou beëindigen c.q. rechtmatig uitschakelen, verduidelijkt dat het CBP overigens geen aanwijzingen heeft dat Vodafone handelt in strijd met de nieuwe netneutraliteitsregels (bijvoorbeeld door niet-netneutrale proposities aan te bieden). De zienswijze 2 van Vodafone heeft op het punt van de 'toekomstige regelgeving' voor het overige niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

### **Vrijheid van ondernemerschap**

Vodafone stelt zich in haar zienswijze 2 op het standpunt dat het CBP zich in strijd met zijn bevoegdheden en de vrijheid van ondernemerschap op detailniveau inlaat met de dagelijkse bedrijfsvoering van Vodafone.

De vrijheid van ondernemerschap omvat de vrijheid om een economische activiteit of een handelsactiviteit uit te oefenen, de contractsvrijheid en de vrije mededinging (artikel 16 van het Handvest).<sup>513</sup> De vrijheid van ondernemerschap heeft echter geen absolute gelding, maar moet in relatie tot haar maatschappelijke functie worden beschouwd.<sup>514</sup> Van belang is of de uitoefening van de ondernemersactiviteit als zodanig wordt belet.<sup>515</sup>

Zoals hierboven gemotiveerd onder het kopje 'Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering', heeft het CBP in het kader van een zorgvuldige kennisvergaring en belangenafweging op conceptueel niveau vastgesteld en in het rapport gemotiveerd hoe de informatiesystemen *zouden kunnen worden vormgegeven*, zonder (te) vergaand in te willen grijpen in de bedrijfsprocessen en bedrijfsvoering van Vodafone door het gebruik van een specifiek(e) product of techniek voor te schrijven.

Het niet zo lang in niet-geanonimiseerde vorm mogen verwerken van de persoonsgegevens, beperkt Vodafone weliswaar bij de inrichting van informatiesystemen. Deze beperking die voortvloeit uit met name de bepalingen van artikel 11.5 van de Tw en overweging 30 van de e-Privacyrichtlijn, verhindert/maakt Vodafone als zodanig niet de uitoefening van haar ondernemersactiviteit onmogelijk, te weten: het aanbieden van een openbare elektronische communicatienetwerk en -dienst.

De zienswijze 2 van Vodafone heeft op het punt van de 'vrijheid van ondernemerschap' ten aanzien van de stelling van het CBP dat met het beginsel van doelbinding samenhangt het beginsel dat persoonsgegevens die voor verschillende doeleinden worden verzameld, gescheiden worden verwerkt (*data siloing*), (wel) aangevuld en verduidelijkt dat het CBP in het rapport daarmee als zodanig (nog) niet het gebruik van een specifiek(e) product of techniek voorschrijft. De zienswijze 2 van

---

<sup>513</sup> HvJ EU 22 januari 2013, zaak C-283/11 (Sky Österreich), r.o. 42. Zie ook URL: <http://www.minbuza.nl/ecer/eu-essentieel/handvest-grondrechten/vrijheden-art.-6-t-m-19/vrijheid-van-ondernemerschap-artikel-16.html> (URL laatst bezocht op 29 mei 2013).

<sup>514</sup> HvJ EG 9 september 2004, gevoegde zaken C184/02 en C223/02 en HvJ EU 6 september 2012, C544/10 (Deutsches Weintor).

<sup>515</sup> HvJ EU 22 januari 2013, zaak C-283/11 (Sky Österreich), r.o. 49.

Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

### **(Schijn van) vooringenomenheid**

(Het vasthouden aan) suggestieve indelingen en beschrijvingen die niet stroken met de werkelijkheid, gezien in combinatie met het feit dat het CBP niet in overleg wil treden met Vodafone en de in de ogen van Vodafone voor het CBP voordelige interpretatie van de wettelijke regels wijst volgens Vodafone op strijd met het verbod van vooringenomenheid (artikel 2:4 van de Awb).

Artikel 2:4, eerste lid, van de Awb bevat de codificatie van de algemene regel dat het bestuursorgaan zijn taak zonder vooringenomenheid dient te vervullen. Daarbij gaat het erom dat de meningsvorming of het handelen van het bestuursorgaan niet mag worden beïnvloed door andere belangen dan die in de voorliggende situatie als relevant kunnen worden beschouwd (fair play).<sup>516</sup> Het is aan de belanghebbende om aan de hand van concrete feiten en omstandigheden een objectief gerechtvaardigde vrees voor vooringenomenheid aannemelijk te maken.<sup>517</sup>

Het CBP wijst er (ten eerste) op dat het rapport steunt op voldoende concrete en objectieve gegevens. Er is geen wettelijk voorschrift of algemeen rechtsbeginsel dat meebrengt dat het rapport geen gedefinieerde termen mag bevatten als bijvoorbeeld 'packet inspection', 'data-analyse technieken' en gegevens 'over' en 'uit' het dataverkeer of een metafoor ter illustratie, zoals die van de brief en de envelop (zie p. 20 van dit rapport). Daar komt bij dat termen als 'gevoelige gegevens', 'persoonsgegevens die ook communicatie betreffen dan wel verkeersgegevens zijn' indelingen zijn die voortvloeien uit de parlementaire geschiedenis.<sup>518</sup>

Het onderzoek van het CBP was (ten tweede) gericht op waarheidsvinding, ofwel het verzamelen van zowel 'belastende' als 'ontlastende' informatie. Zo heeft het CBP kennis vergaard over zowel de werkwijze van Vodafone bij de inzet van data-analyse technieken, de noodzaak daartoe (bijvoorbeeld op het punt van de netwerkbelasting en de verwachte toename daarvan) en mogelijke alternatieven.

Zoals hierboven gemotiveerd onder het kopje 'Fair play- en lex certa-beginsel: geen overleg over beëindigen geconstateerde overtredingen', is er geen wettelijk voorschrift of algemeen rechtsbeginsel dat meebrengt dat een toezichthouder gehouden is om met een overtreder, samen te bezien hoe de overtreder geconstateerde overtredingen kan beëindigen. De weigering om met Vodafone te 'overleggen' over hoe de geconstateerde kunnen worden beëindigd, kunnen dan ook niet worden beschouwd als concrete feiten en omstandigheden waaruit een objectief gerechtvaardigde vrees voor vooringenomenheid kan worden afgeleid.

---

<sup>516</sup> *Commentaar Algemeen Bestuursrecht*, artikel 2:4 Awb, aantekening 1.1.

<sup>517</sup> Zie o.a. AbRvS 10 juli 2002, LfN AE5120 en AbRvS 14 maart 2012, LfN BV8750. Vgl. No 11 mei 2011, AB 2011, 270.

*Commentaar Algemeen Bestuursrecht*, artikel 2:4 Awb, aantekening 1.7.

<sup>518</sup> Zie o.a. *Kamerstukken II* 2000/01, 27 460, nr. 1, p. 27; *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61; *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 59: "Voor zover verkeersgegevens zijn aan te merken als persoonsgegevens".

Het CBP bestrijdt verder (nogmaals) dat het wettelijk kader niet tegen een neutrale achtergrond is gepresenteerd. Vodafone heeft (ook) op dit punt volgens het CBP te weinig gesteld om een objectief gerechtvaardigde vrees voor vooringenomenheid aannemelijk te maken. Er zijn eerder aanwijzingen voor het tegenovergestelde. In dit verband wijst het CBP erop dat bijvoorbeeld toetsing aan louter de 'grondslagen' in de Tw, zoals voorgestaan door Vodafone, niet leidt tot een andere uitkomst dan de toetsing uitgevoerd door het CBP, zodat van strijd met het beginsel van fair play/(schijn van) vooringenomenheid geen sprake kan zijn.

Ook het feit dat de zienswijzen 1 en 2 van Vodafone hebben geleid tot wijziging van het (Concept)rapport definitieve bevindingen, duidt niet op vooringenomenheid.

Niet valt (bovendien) in te zien waarom de omstandigheid dat er inmiddels netneutraliteitswetgeving is, maakt dat het onderzoek moet worden beëindigd. Nog daargelaten de onderzoeksplicht van het CBP vanwege de informatieverstrekking door OPTA aan het CBP (zie hierover verder het kopje 'Samenwerkingsafspraken van het CBP met respectievelijk de ACM en AT').

De zienswijze 2 van Vodafone heeft op het punt van (het gebruik van) het OSI-model en (de werkwijze van Vodafone bij) de inzet van data-analyse technieken (zie p. 137 van dit rapport, bullet points (iv) tot en met (viii) en (x)) (desondanks) geleid tot verduidelijking en aanpassing van de feitelijke bevindingen in het rapport.

De zienswijze 2 van Vodafone heeft op het punt van de door het CBP aangehaalde initiatieven en activiteiten om netwerkaanbieders te helpen om te gaan met het grotere aantal signaleringen als gevolg van smartphones en apps (zie p. 137 van dit rapport, bullet point (ix)) geleid tot nuancering van het belang van de relativering door BEREC van de toename in dataverkeer en andere initiatieven om de druk op het signaleringskanaal te verminderen.

Daarnaast is uit zorgvuldigheid en om misverstanden te voorkomen [VERTROUWELIJK] weggelaten uit dit Rapport definitieve bevindingen.

De zienswijze 2 van Vodafone heeft op de hierboven genoemde punten niet geleid tot aanpassing van de conclusies in het rapport. De zienswijze 2 van Vodafone heeft op dit punt van de '(schijn van) vooringenomenheid' voor het overige niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

### **Opzet en structuur rapport**

Vodafone maakt in haar zienswijze 2 opmerkingen over het feit dat het Conceptrapport definitieve bevindingen volgens haar inconsistent is van opzet en structuur, waarbij feiten, juridisch kader en beoordeling door elkaar lopen.

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

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

Het CBP bestrijdt dat het wettelijk kader niet tegen een neutrale achtergrond is gepresenteerd. Bijvoorbeeld toetsing aan louter de 'grondslagen' in de Tw, zoals voorgestaan door Vodafone, leidt niet tot een andere uitkomst dan de toetsing uitgevoerd door het CBP, zodat van strijd met het beginsel van fair play/(schijn van) vooringenomenheid (artikel 2:4 van de Awb) geen sprake kan zijn (zie ook het kopje 'Samenloop Wbp en Tw').

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

De zienswijze 2 van Vodafone heeft op het punt van de opzet en structuur voor het overige niet geleid tot aanpassing van het rapport.

#### Geen overtreding van privacyregels: opmerkingen en aanvullingen feitelijk kader

**Zienswijze 2 Vodafone:** Vodafone meent dat zij op geen enkele wijze de Wbp of de Tw heeft overtreden of overtreedt (zij verwijst daarbij ook naar haar zienswijze 1). Ten onrechte heeft deze zienswijze 1 van Vodafone niet geleid tot aanpassing van de conclusies van het CBP omtrent de naleving van de privacyregels. Vodafone merkt in haar zienswijze 2 (samengevat) op dat:

- **het Conceptrapport definitieve bevindingen een aantal wezenlijke feitelijke/technische misvattingen bevat.**

Vodafone verwijst in dat verband (kort gezegd) naar de volgende aspecten/elementen:

- (i) Vodafone maakt voor wat betreft netwerk(en)opbouw een onderscheid (op technologie): 2G voor voice en GPRS dataverkeer en 3G voor voice en UMTS dataverkeer;<sup>519</sup>
- (ii) bij zogenaamde chatty apps vindt geen 'uitwisseling' van dataverkeer of gegevens plaats met de zendmasten (door Vodafone), er vindt slechts 'verkeer' plaats, via een app;<sup>520</sup>
- (iii) het CBP geeft in Hoofdstuk 1 (Inleiding) van het Conceptrapport definitieve bevindingen een te beperkte definitie of omschrijving van netwerkbeheer;<sup>521</sup>
- (iv) het CBP noemt in Hoofdstuk 1 (Inleiding) van het Conceptrapport definitieve bevindingen legitieme, ruime bedrijfsdoeleinden (die de

---

<sup>519</sup> Zienswijze 2 Vodafone, p. 12.

<sup>520</sup> Idem, p. 13.

<sup>521</sup> Idem.

- eindgebruiker dienen) die door de inzet van een breed scala technieken, *waaronder* ‘packet inspection’ worden nagestreefd;<sup>522</sup>
- (v) het CBP meldt - ten onrechte - niet dat OPTA in het in mei en juni 2011 uitgevoerde onderzoek betreffende data-analyse technieken geen overtreding heeft geconstateerd;<sup>523</sup>
  - (vi) het CBP meldt in Hoofdstuk 1 (Inleiding) van het Conceptrapport definitieve bevindingen als het gaat om het verloop van het onderzoek - ten onrechte - niet over welke onderwerpen en met welke reden Vodafone heeft verzocht met het CBP in overleg te treden;<sup>524</sup>
  - (vii) Vodafone betwist de relevantie van het (concept) BEREC-rapport dat niet ziet op data-analyse technieken, maar een rapport over netneutraliteit is en geschreven vanuit een economische, en niet een technische achtergrond;<sup>525</sup>
  - (viii) het gebruik van signaleringskanalen is gerelateerd aan het opzetten van een verbinding. Smartphones verbreken de verbinding veelvuldig om de batterij te sparen. Gevolg daarvan is dat ook vaak weer verbinding wordt gezocht met het netwerk, om data van de server af te halen of te checken of er updates beschikbaar zijn. Daarbij gaat een signalering gepaard. Er is dus een sterke relatie tussen het applicatiegedrag en de wijze waarop het netwerk belast wordt, wat operators in kaart willen brengen om de integriteit en stabiliteit van het netwerk te kunnen bewaren;<sup>526</sup>
  - (ix) (onder verwijzing naar haar zienswijze 1:) Vodafone verwerkt niet altijd op individueel klantniveau gegevens om valide, bruikbare informatie te krijgen over de netwerkbelasting als gevolg van de toename van dataverkeer, maar alleen met de [VERTROUWELIJK: apparatuur]: om storingen tijdig te kunnen oplossen en om (na uitdrukkelijke toestemming) vragen en klachten van klanten te kunnen behandelen en verhelpen (waarbij Vodafone overigens opmerkt ‘dat het haar ondernemersvrijheid raakt’);<sup>527</sup>
  - (x) (onder verwijzing naar haar zienswijze 1 over de [VERTROUWELIJK: apparatuur]: [VERTROUWELIJK]
  - (xi) (onder verwijzing naar haar zienswijze 1 en e-mail van 10 juli 2012 over de [VERTROUWELIJK: apparatuur] en de [VERTROUWELIJK: apparatuur]:) [VERTROUWELIJK]
  - (xii) (onder verwijzing naar haar zienswijze 1 en e-mail van 10 juli 2012 over de [VERTROUWELIJK: apparatuur]:) [VERTROUWELIJK]
  - (xiii) (over de [VERTROUWELIJK: apparatuur]:) er wordt per categorie opgeslagen, niet per abonnee.<sup>528</sup> Vodafone kan de ruwe data niet benaderen;<sup>529</sup>

---

<sup>522</sup> Idem, p. 13-14.

<sup>523</sup> Idem, p. 14.

<sup>524</sup> Idem, p. 19-20.

<sup>525</sup> Idem, p. 24 en 30.

<sup>526</sup> Idem, p. 26-27.

<sup>527</sup> Idem, p. 26-27 en 30 en 54.

<sup>528</sup> Zienswijze 2 Vodafone, p. 35 en 56.

<sup>529</sup> Idem, p. 64.

- (xiv) (onder verwijzing naar haar zienswijze 1 over de [VERTROUWELIJK: apparatuur]:) locatie-informatie in de [VERTROUWELIJK: apparatuur] is gegenereerd door (2G-)spraakverkeer, niet door data-verkeer, zodat deze data buiten de reikwijdte van het onderzoek valt. De in het Conceptrapport definitieve bevindingen genoemde bewaartermijnen ten aanzien van de 15-minuten rapporten, dagrapporten en weekrapporten zijn onjuist: de weekrapporten worden slechts zes maanden bewaard;<sup>530</sup>
- (xv) Vodafone is bereid haar Privacy Statement aan te passen met informatie over spamfiltering, virus- en malwarebestrijding. Vodafone merkt op dat zij, naast het feit dat haar Privacy Statement is gewijzigd, onder andere een Privacy Web Center heeft ingericht, met daarop informatie over de wijze waarop Vodafone omgaat met privacy, en waarin uitdrukkelijk ook wordt ingegaan op data-analyse technieken/spamfiltering, virus- en malwarebestrijding;<sup>531</sup>
- (xvi) Vodafone bestrijdt dat de uitkomsten van netwerkstatistieken niet minder representatief worden voor het Vodafone abonneebestand wanneer de gegevens van die ene specifieke individuele betrokkene niet worden meegenomen. Als zij gegevens van alle ‘specifieke’ abonnees niet mag meenemen, is van representativiteit geen sprake;<sup>532</sup>
- (xvii) [VERTROUWELIJK]
- (xviii) steekproefsgewijze toetsing van gegevens is volgens Vodafone technisch niet mogelijk;<sup>533</sup>
- (xix) voor de [VERTROUWELIJK: apparatuur] zijn de bewaartermijnen voor het doeleinde van ‘actueel verkeersbeheer’ niet anders dan de termijnen voor ‘netwerkcapaciteitsplanningen’;<sup>534</sup>
- (xx) in haar reactie op de vordering van het CBP geeft Vodafone inzicht in de volgens haar voor de [VERTROUWELIJK: apparatuur] noodzakelijke bewaartermijnen. [VERTROUWELIJK]

- **er geen andere, minder ingrijpende middelen bestaan om het zelfde resultaat te bereiken.**

- (i) Het CBP is er aan voorbij gegaan dat één van leveranciers ([VERTROUWELIJK]) in het kader van de zienswijze 1 van Vodafone al heeft verklaard dat een dergelijke aanpassing geen lichtere ‘inbreuk’ oplevert, maar wel een significante verslechtering van de dienstverlening zal betekenen (eerder anonimiseren is ook niet mogelijk volgens deze leverancier).<sup>535</sup> Het CBP miskent dat de [VERTROUWELIJK: apparatuur] in de huidige configuratie absoluut noodzakelijk is voor de stabiliteit en integriteit van het netwerk, het oplossen van klantklachten alsmede

<sup>530</sup> Zienswijze 2 Vodafone, p. 35-36.

<sup>531</sup> Idem, p. 37-38.

<sup>532</sup> Idem, p. 54.

<sup>533</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 11.

<sup>534</sup> Idem, p. 12.

<sup>535</sup> Zienswijze 2 Vodafone, p. 9, 57 en 65. Reactie Vodafone op vordering van 21 februari 2013, p. 9. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 10.



nakoming van bestaande overeenkomsten.<sup>536</sup> Het CBP miskent verder dat ten aanzien van de [VERTROUWELIJK: apparatuur] een lichtere verwerkingsmaatregel dan de huidige één-uurs anonimisering niet kan worden geïmplementeerd (minimale duur om de gegevens vanuit het core netwerk te categoriseren en anonimiseren), zonder een geheel nieuw product te (laten) ontwikkelen (waarvan niet eens duidelijk is of dit mogelijk is, wat disproportioneel kostbaar zal zijn, terwijl de impact op de privacy van de eindgebruiker verwaarloosbaar is).<sup>537</sup> Volgens de leverancier van de [VERTROUWELIJK: apparatuur] is de verwerking ook in overeenstemming met vigerende privaceregels.<sup>538</sup> Ten slotte is (ook) de lichtere maatregel die het CBP mogelijk acht ten aanzien van het opwaarderen van prepaid tegoed onbewezen, waarbij geldt dat Vodafone het opwaarderen van prepaid tegoed thans zodanig aanbiedt als het CBP in het Rapport voorlopige bevindingen aanhing.<sup>539</sup>

- (ii) Mobiel bellen heeft de facto de functie van universele dienst van vast bellen overgenomen. Continuïteit van de dienstverlening en een altijd werkend (dus kwalitatief hoogwaardig) netwerk zijn een primaire doelstelling die kan worden afgedwongen door de overheid. Hiervoor is informatie op individueel klantniveau noodzakelijk. In het bijzonder voor dit doeleinde gebruikt Vodafone de [VERTROUWELIJK: apparatuur].<sup>540</sup>
- (iii) Vanwege het evenredigheidsbeginsel (netwerkinfficiënt, kostbaar en leidt tot onnodige energieverstopping) en het beginsel van dataminimalisatie kan niet van Vodafone worden geëist dat zij per doeleinde zelfstandige apparaten voor de verwerking installeert.<sup>541</sup>
- (iv) Vodafone geeft in haar zienswijze 2 nog een aantal voorbeelden om de noodzakelijkheid van de [VERTROUWELIJK: apparatuur] in zijn huidige vorm aan te tonen, juist voor netwerkbeheer (vroegtijdig signaleren van netwerkproblemen<sup>542</sup>). [VERTROUWELIJK]
- (v) Vodafone voegt daaraan toe dat [VERTROUWELIJK]
- (vi) [VERTROUWELIJK]

### **Algemene opmerkingen en aanvullingen**

**Reactie CBP:** Vodafone merkt in haar zienswijze 2 op dat het Conceptrapport definitieve bevindingen nog een aantal feitelijke/technische onjuistheden bevat.

De zienswijze 2 van Vodafone heeft op dit punt (zie p. 153 e.v. van dit rapport, bullet points (i) tot en met (viii), (xi), (xiii) tot en met (xvi) en (xviii) tot en met (xx)) geleid tot aanvulling en aanpassing van de feitelijke bevindingen in het rapport. Ten aanzien van de bullet points (ix), (x), (xii) en (xvii) heeft de zienswijze 2 van Vodafone ook

<sup>536</sup> Zienswijze 2 Vodafone, p. 9. Reactie Vodafone op vordering van 21 februari 2013, p. 15-17.

<sup>537</sup> Zienswijze 2 Vodafone, p. 10, 55-56 en 65. Reactie Vodafone op vordering van 21 februari 2013, p. 10.

<sup>538</sup> Reactie Vodafone op vordering van 21 februari 2013, p. 9.

<sup>539</sup> Zienswijze 2 Vodafone, p. 10.

<sup>540</sup> Idem, p. 26.

<sup>541</sup> Idem, p. 27-28 en 66.

<sup>542</sup> Zie idem, p. 57

geleid tot aanvulling en aanpassing van de feitelijke bevindingen, maar met de volgende kanttekeningen:

- ad (ix): hoewel het juist is dat Vodafone om valide, bruikbare informatie te krijgen over de netwerkbelasting als gevolg van de toename van dataverkeer niet in alle verwerkingsstadia verkeersgegevens verwerkt die ook persoonsgegevens zijn, zijn de gegevens ten tijde van het verzamelen daarvan alle (nog) herleidbaar tot de betrokken abonnees (zie paragraaf 3.3, p. 50 e.v. van dit rapport);
- ad (x) en (xvii): de omstandigheid dat in de [VERTROUWELIJK: apparatuur] gegevens op [VERTROUWELIJK] worden bewaard en verwerkt en niet 'bezoek en gebruik' op een hoger abstractieniveau, ingedeeld per abonnee, doet er niet aan af dat de verwerkte gegevens (dan) nog herleidbaar zijn tot de betrokken abonnees;
- ad (xii): anders dan Vodafone meent, worden voor het verkrijgen van data over het opzetten van een datasessie (netwerk signaleringsdata) via de [VERTROUWELIJK: apparatuur] wel degelijk data-analyse technieken ingezet: het gaat in alle gevallen om datapakketten.
- ad (xvii): Vodafone heeft zich op het standpunt gesteld dat de verzamelde informatie in zijn totaliteit nodig is om een inschatting te kunnen geven van de op termijn benodigde netwerkcapaciteit: niet gezegd of geoordeeld kan worden dat soorten gegevens 'per stuk' noodzakelijk zijn of kunnen zijn, maar dat het gaat om de samenhang van gegevens die slechts in combinatie met elkaar relevante informatie opleveren uit het netwerk en daarmee dus in samenhang relevant zijn.<sup>543</sup> Voor zover Vodafone hieraan heeft toegevoegd dat de categorieën van gegevens zich overigens ook niet laten scheiden vanwege de configuratie-instellingen van de data-analyse apparatuur die Vodafone inzet, wijst het CBP op het volgende. Het CBP heeft (aanvullende) inlichtingen van Vodafone *gevorderd* omtrent de vraag welke categorieën van niet-geanonimiseerde gegevens over en/of uit het mobiele dataverkeer noodzakelijkerwijs moeten worden gebruikt om voor het doeleinde van verkeersbeheer (meer in het bijzonder, netwerkplanning) een inschatting van de op termijn benodigde netwerkcapaciteit te kunnen maken. Het CBP heeft daaraan toegevoegd: *"Het CBP verwacht dat u bij de beantwoording van deze vraag en de volgende vragen, tenzij expliciet anders is vermeld, abstraheert van (de configuratie-instellingen op) de thans bij u in gebruik zijnde data-analyse apparatuur. (...)"*, (onderstreping toegevoegd door het CBP).<sup>544</sup> In een telefoongesprek met medewerkers en de advocaat-gemachtigde van Vodafone op 14 januari 2013 hebben medewerkers van het CBP toegelicht dat 'abstraheren van configuratie-instellingen' betekent dat wordt gevraagd het antwoord los te koppelen van de beslissing om deze data-analyse apparatuur te kopen (oftewel, te abstraheren van de mogelijke beperkingen van de betreffende apparatuur). De hierboven weergegeven verklaring van Vodafone dat de categorieën van gegevens zich ook niet laten scheiden vanwege de configuratie-instellingen van de data-analyse apparatuur die Vodafone inzet is (dan ook) op zich nog geen tegenbewijs voor de stelling van het CBP dat er andere, minder ingrijpende middelen zijn om het zelfde resultaat te bereiken

---

<sup>543</sup> Idem, p. 8.

<sup>544</sup> Vordering CBP inlichtingen en inzage in zakelijke gegevens en bescheiden van 20 december 2012 en herstellvordering CBP van 7 maart 2013.

en evenmin bewijs voor de stelling dat haar belang door het niet zo lang in niet-geanonimiseerde vorm mogen verwerken van de persoonsgegevens onevenredig is geschaad.

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer (meer in het bijzonder: netwerkplanning) via de [VERTROUWELIJK: apparatuur] geleid tot aanpassing van de conclusies in het rapport.

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer (meer in het bijzonder: netwerkmonitoring) via de [VERTROUWELIJK: apparatuur] gedeeltelijk geleid tot aanpassing van de conclusies in het rapport (zie hierover verder het kopje 'Geen andere, minder ingrijpende middelen om het zelfde resultaat te bereiken' hieronder).

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens voor het doeleinde behandeling van verzoeken om inlichtingen van klanten geleid tot aanpassing van de conclusies in het rapport.

De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de conclusies in het rapport.

#### **Geen andere, minder ingrijpende middelen om het zelfde resultaat te bereiken**

Vodafone stelt zich in haar zienswijze 2 op het standpunt dat er geen andere, minder ingrijpende middelen zijn om het zelfde resultaat te bereiken.

De zienswijze 2 van Vodafone heeft op dit punt (zie p. 156 e.v. van dit rapport, bullet points (ii) tot en met (vi)) geleid tot aanvulling en aanpassing van de feitelijke bevindingen in het rapport. Ten aanzien van de bullet point (i) heeft de zienswijze 2 van Vodafone ook geleid tot aanvulling en aanpassing van de feitelijke bevindingen, maar met de volgende kanttekeningen: in haar zienswijze 1 heeft Vodafone tegenbewijs geleverd door overlegging van een verklaring van haar leverancier [VERTROUWELIJK] dat het concrete voorbeeld van het CBP geen lichtere maatregel is (maar wel een significante verslechtering van de dienstverlening zal betekenen).<sup>545</sup> Gelet daarop is dit concrete voorbeeld niet gehandhaafd in het Conceptrapport definitieve bevindingen. De door het CBP gestelde alternatieve maatregel die inhoudt dat toegang wordt verleend tot een beperkte hoeveelheid gratis (https) dataverkeer, waarmee de prepaid abonnee een opwaardeer-/betalingswebsite kan bezoeken voor het 'subdoeleinde' het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites, heeft Vodafone in haar zienswijze 2 onvoldoende onderbouwd weersproken (zie hierover verder het kopje 'Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering').

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde

---

<sup>545</sup> Bijlage 2 bij Zienswijze 1 Vodafone: "[VERTROUWELIJK]."

verkeersbeheer (meer in het bijzonder: netwerkplanning) via de [VERTROUWELIJK: apparatuur] geleid tot aanpassing van de conclusies in het rapport.

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer (meer in het bijzonder: netwerkmonitoring) via de [VERTROUWELIJK: apparatuur] gedeeltelijk geleid tot aanpassing van de conclusies in het rapport. Voor wat betreft de zes-maanden geaggregeerde data ([VERTROUWELIJK: identifier]) die Vodafone bewaart en verwerkt om trends in haar netwerk te onderkennen, bijvoorbeeld problemen in verband met OS-updates ([VERTROUWELIJK]), wijst het CBP op het volgende. Nu Vodafone in haar zienswijze 2 aannemelijk maakt dat zij onder andere aan de hand van [VERTROUWELIJK] problemen in verband met OS-updates moet kunnen signaleren, valt niet in te zien waarom Vodafone voor dat doel niet zou kunnen volstaan met het bewaren en verwerken van de [VERTROUWELIJK]. Dit in plaats van het volledige [VERTROUWELIJK: identifier], te bewaren en verwerken dat (de grootste) identificeerbaarheid meebrengt, omdat het op zichzelf persoonsidentificerende kenmerken bevat, ook zonder de onderlinge combinatie of in samenhang met uit andere bron bekende informatie (zie hierover verder p. 83 e.v. van dit rapport).

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens voor het doeleinde behandeling van verzoeken om inlichtingen van klanten geleid tot aanpassing van de conclusies in het rapport.

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het ‘subdoeleinde’ het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed geleid tot aanpassing van de conclusies in het rapport.

De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de conclusies in het rapport.

#### Opmerkingen wettelijk kader

##### *Samenloop Wbp en Tw*

**Zienswijze 2 Vodafone:** Vodafone stelt zich in haar zienswijze 2 (onder andere onder verwijzing naar de wetsgeschiedenis en de tekst van het samenwerkingsprotocol CBP-OPTA, en in reactie op een in de ogen van Vodafone voor het CBP voordelige interpretatie van de wettelijke regels) op het standpunt dat de Wbp geen rol speelt voor zover nadere uitwerking van de normen heeft plaatsgevonden in de Tw. Waar het verkeersgegevens betreft, kan volgens Vodafone aan een beoordeling van de Wbp niet worden toegekomen, omdat de nadere uitwerking daarvan in hoofdstuk 11 van de Tw staat.<sup>546</sup> Voor zover Vodafone ook persoonsgegevens verwerkt die geen verkeersgegevens zouden zijn (wellicht het geval bij spyware, malware, virussen,

---

<sup>546</sup> Zienswijze 2 Vodafone, p. 14-16, 49, 52-53 en 63-64.

spam etc.) heeft Vodafone een geldige Wbp-grondslag.<sup>547</sup> Zodra een verwerking voldoet aan artikel 11.2a van de Tw, kan geen sprake zijn van strijd met de Wbp.<sup>548</sup>

**Reactie CBP:** Het CBP wijst erop dat de e-Privacyrichtlijn (geïmplementeerd in de Tw) zich verhoudt tot de Privacyrichtlijn (geïmplementeerd in de Wbp) als sectorale tot algemene regels.<sup>549</sup> De richtlijnen hebben (deels) een ander karakter<sup>550</sup> en een ander toepassingsbereik. Dat wil zeggen dat - anders dan de Privacyrichtlijn - de e-Privacyrichtlijn ook van toepassing is op de verwerking van verkeersgegevens die geen persoonsgegevens zijn (gegevens van rechtspersonen). Anders dan de e-Privacyrichtlijn, geldt de Privacyrichtlijn ook voor zover het gaat om de verwerking van verkeersgegevens die ook persoonsgegevens zijn in niet openbare elektronische communicatienetwerken en -diensten. Op dezelfde manier is de verhouding tussen de Tw en de Wbp er een van (aanvullende) sectorale normen naast - en niet in plaats van - de Wbp.<sup>551</sup> Er is in algemene zin geen sprake van een lex specialis-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene. Wel geldt dat indien en voor zover de e-Privacyrichtlijn (als geïmplementeerd in de Tw) ten aanzien van de verwerking van persoonsgegevens op een bepaald punt een uitputtende regeling bevat, die regeling voorgaat op de algemene normen uit de Privacyrichtlijn (als geïmplementeerd in de Wbp).<sup>552</sup>

Artikel 11.5 van de Tw vormt een implementatie van artikel 6 van de e-Privacyrichtlijn en geeft regels voor de verwerking van verkeersgegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten. Uit de wetsgeschiedenis bij de Tw blijkt dat artikel 11.5 van de Tw (weliswaar) 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.”*<sup>553</sup>

Voor het verwerken van persoonsgegevens is (desondanks) een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8 van de Wbp. Uit de wetsgeschiedenis bij de Wbp kan wel worden afgeleid dat artikel 8 van de Wbp een uitputtende opsomming geeft van verwerkingsgronden: *“Artikel 7 betreft de verzameling van persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en*

---

<sup>547</sup> Idem, p. 47, 52-53 en 64.

<sup>548</sup> Idem, p. 64.

<sup>549</sup> Uit de tekst van artikel 3, eerste lid, van de Privacyrichtlijn volgt dat deze een algemeen - niet sectoraal - toepassingsbereik heeft. De algemene Privacyrichtlijn is daarom mede van toepassing op de verwerking van persoonsgegevens in de telecommunicatiesector. Zie ook *Kamerstukken II 1996/97*, 25 533, nr. 3, p. 13. Uit de tekst van artikel 1, tweede lid, van de telecomspecifieke e-Privacyrichtlijn volgt dat de bepalingen van deze richtlijn ‘een specificatie van en een aanvulling’ vormen op de Privacyrichtlijn. Zie in dezelfde zin overweging 10, 12, 20, laatste volzin, en 46 en artikel 4, eerste lid bis, van de e-Privacyrichtlijn.

<sup>550</sup> Bijvoorbeeld: de bepalingen in de e-Privacyrichtlijn die betrekking hebben op de beschikbaarheid van nummeridentificatie. Vgl. *Kamerstukken II 2002/03*, 28 851, nr. 7, p. 54.

<sup>551</sup> *Kamerstukken II 1999/2000*, 26 410, nr. 7, p. 2. Zie in dat verband ook *Kamerstukken II 2002/03*, 28 851, nr. 7, p. 78-79.

<sup>552</sup> Zie ook *Kamerstukken II 2002/03*, 28 851, nr. 3, p. 45.

<sup>553</sup> *Kamerstukken II 2002/03*, 28 851, nr. 7, p. 54. Zie ook *Kamerstukken II 2002/03*, 28 851, nr. 3, p. 59.

*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.”*<sup>554</sup>

Als hoofdregel geldt op grond van dit artikel 11.5 van de Tw dat alle door aanbieders van openbare communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens moeten worden verwijderd of geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. Op deze hoofdregel zijn in de leden 2 en 3 van het artikel uitzonderingen geformuleerd (bijvoorbeeld voor verkeersgegevens die noodzakelijk zijn voor facturering, of voor marktonderzoek/verkoopactiviteiten en toegevoegde waardediensten mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor toestemming heeft gegeven).<sup>555</sup>

Artikel 11.5 van de Tw geeft aldus een telecomspecifieke uitwerking van artikel 10 van de Wbp<sup>556</sup> op het punt van de bevoegdheid tot (toelaatbaarheid van) het bewaren van persoonsgegevens die ook verkeersgegevens zijn (oftewel, een verplichting tot verwijdering dan wel anonimisering van gegevens, met uitzonderingen).<sup>557</sup> 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).<sup>558</sup> Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.5 van de Tw genoemde (uitgezonderde) verwerkingsdoelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp.

---

<sup>554</sup> *Kamerstukken II 1998/99, 25 892, nr. 13, p. 5-6.*

<sup>555</sup> Onder ‘overbrenging van communicatie’ en ‘facturering’ moet ook verkeersbeheer, behandeling van verzoeken om inlichtingen van abonnees en opsporing van fraude worden begrepen (artikel 11.5, vijfde lid, van de Tw). De verkeersgegevens mogen (ook) voor die (afgeleide) verwerkingsdoelen worden verwerkt, voor zover noodzakelijk.

<sup>556</sup> Te weten: het vereiste dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (bewaartermijn).

<sup>557</sup> *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.

<sup>558</sup> 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.*

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

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

Artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) geeft een verplichting voor de aanbieders van openbare elektronische communicatienetwerken en -diensten om passende en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (zorgplicht internetveiligheid). Dit artikel stelt eisen aan de beveiliging van persoonsgegevens en geeft aldus een telecomspecifieke uitwerking van artikel 13 van de Wbp.<sup>559</sup> Het artikel geeft (dus) op zichzelf geen grondslag voor de verwerking van persoonsgegevens die ook communicatie betreffen.

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

Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de in artikel 11.3 en/of artikel 11.2a van de Tw genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. Dat daargelaten, geeft de regeling in artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en artikel 5 van de e-Privacyrichtlijn

---

<sup>559</sup> 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.

(geïmplementeerd in artikel 11.2a van de Tw) een nadere begrenzing/inperking van de toegestane verwerkingen van persoonsgegevens die ook communicatie betreffen in de telecommunicatiesector, namelijk waar het gaat om de vraag of daarvoor een grondslag is te vinden in de Wbp. Het CBP heeft de beoordeling van de grondslag voor het verwerken van persoonsgegevens die ook communicatie betreffen derhalve getoetst aan artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) jo. artikel 8 van de Wbp. Materieel (inhoudelijk) betekent dat als de gegevensverwerking is toegestaan onder artikel 4 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.3 van de Tw) en/of artikel 5 van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.2a van de Tw) ook een bijbehorende grondslag is te vinden als opgesomd in artikel 8 van de Wbp en - omgekeerd - als de verwerking niet is toegestaan onder de e-Privacyrichtlijn/Tw ook geen grondslag is te vinden in de Wbp.

Ten overvloede wijst het CBP erop dat toetsing aan louter de ‘grondslagen’ in de Tw, zoals voorgestaan door Vodafone, niet leidt tot een andere uitkomst dan de toetsing uitgevoerd door het CBP, zodat van strijd met het beginsel van fair play/(schijn van) vooringenomenheid (artikel 2:4 van de Awb) geen sprake kan zijn.

De zienswijze 2 van Vodafone heeft op het punt van de samenloop van Wbp en Tw, meer in het bijzonder de toetsing van de grondslag voor (i) de verwerking van persoonsgegevens die ook verkeersgegevens zijn en (ii) de verwerking van communicatie, tevens persoonsgegevens, geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

#### *Bevoegdheid CBP*

**Zienswijze 2 Vodafone:** Vodafone stelt zich in haar zienswijze 2 (kort gezegd) op het standpunt dat:

- (i) de toezichthoudende taak van het CBP is beperkt tot het terrein van de Wbp en zich niet uitstrekt tot de Tw;<sup>560</sup>
- (ii) het CBP een wettelijke bevoegdheid ontbeert om onderzoek te doen naar mogelijke overtreding van andere normen dan neergelegd in de Wbp;<sup>561</sup> en/of
- (iii) het onderzoek op grond van de samenwerkingsafspraken van het CBP met OPTA en Agentschap Telecom zou moeten worden uitgevoerd door OPTA respectievelijk AT.<sup>562</sup>

#### **Toezichthoudende taak van het CBP**

**Reactie CBP:** Volgens artikel 51, eerste lid, van de Wbp heeft het CBP onder andere “tot taak (...) toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde.” Artikel 61, eerste lid, van de Wbp regelt dat met het toezicht op de naleving als bedoeld in artikel 51, eerste lid, van de Wbp onder andere zijn belast de collegeleden en de ambtenaren van het secretariaat van het CBP.

---

<sup>560</sup> Zienswijze 2 Vodafone, p. 10, 16, 53-54 en 66.

<sup>561</sup> Idem, p. 16-17, 51 en 53.

<sup>562</sup> Idem, 16-18 en 53.



Waar in de Wbp de term ‘bij en krachtens de wet’ wordt gebruikt, wordt in algemene zin verwezen naar wetten, algemene maatregelen van bestuur en andere regelingen op grond waarvan persoonsgegevens worden verwerkt.<sup>563</sup>

Uit de wetsgeschiedenis bij de Wbp blijkt dat de wetgever met de zinsnede ‘bij en krachtens de wet’ heeft bedoeld dat *“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. Aan het Cbp is daartoe op grond van hoofdstuk 10 van het wetsvoorstel een aantal handhavingsbevoegdheden toegekend. Dit stelsel van toezicht en handhaving staat naast artikel 15.1, derde lid, van het voorstel voor een Telecommunicatiewet, op grond waarvan de OPTA een algemene toezichts- en handhavingsbevoegdheid heeft. De OPTA is ook belast met toezicht op de naleving en de bestuursrechtelijke handhaving van hoofdstuk 11. Die bevoegdheden zullen met name betekenis hebben voor zover het niet de verwerking van persoonsgegevens betreft”*, (onderstreping toegevoegd door het CBP).<sup>564</sup> In de wetsgeschiedenis bij de Tw is voorts opgemerkt dat *“het CBP (...) op grond van de Wbp [is, toevoeging door het CBP] 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 de 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”*<sup>565</sup>

Zie in dezelfde zin de Minister van Economische Zaken in de memorie van antwoord bij het wetsvoorstel tot wijziging van de Tw in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten (Kamerstukken II 2002/03-2003/04, 28 851) in reactie op vragen over de taakverdeling tussen het CBP en OPTA die door Vodafone waren gesteld in een brief van 4 december 2003: *“In zijn brief stelt Vodafone tenslotte nog enkele vragen met betrekking tot de taakverdeling van het CBP en OPTA bij privacy aangelegenheden. Alvorens daarop in te gaan, wens ik eerst te reageren op een enkele - niet onbelangrijke - opmerking van Vodafone in de toelichting op die vragen, namelijk dat nu - onder de nieuwe wet - ook OPTA bevoegdheden krijgt voor toezicht op de privacy. Het CBP, aldus Vodafone, had deze bevoegdheid al langer en het ontstane «dubbele» toezicht zou onzekerheid veroorzaken in de sector. Dit is een uitermate curieuze opmerking van Vodafone, nu immers het college reeds sinds de totstandkoming van de Telecommunicatiewet in 1998 expliciet met het toezicht op de privacybepalingen van hoofdstuk 11 van de Telecommunicatiewet is belast. Al die tijd is daarnaast het CBP - voorheen de Registratiekamer - eveneens bevoegd geweest waar het gaat om de verwerking van persoonsgegevens in de*

<sup>563</sup> Ingevolge aanwijzing 83a, eerste lid, van de Aanwijzingen voor de regelgeving wordt de term ‘deze wet’ gehanteerd bij verwijzing naar een ander onderdeel van de wet zelf waarin de verwijzing is opgenomen. Daar is in dit geval geen sprake van. De term ‘de wet’ is in de Wbp evenmin gedefinieerd als ‘Wbp’.

<sup>564</sup> Kamerstukken II 1998/99, 25 892, nr. 6, p. 43.

<sup>565</sup> Kamerstukken II 2002/03, 28 851, nr. 3, p. 61.

*telecomsector. Er bestaat dus al meer dan vijf jaar een situatie van «dubbel» toezicht. (...)», (onderstreping toegevoegd door het CBP).<sup>566</sup>*

Noch de tekst van de bepalingen noch de wetsgeschiedenis biedt daarom steun voor de opvatting van Vodafone dat de toezichthoudende taak van het CBP is beperkt tot het terrein van de Wbp en zich niet uitstrekt tot hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie.

Anders dan Vodafone betoogt, is het CBP op grond van artikel 51, eerste lid, van de Wbp wel degelijk belast met het houden van toezicht op zowel de naleving van het bepaalde bij of krachtens de Wbp als van hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegevens door aanbieders van openbare elektronische communicatienetwerken en -diensten. De collegeleden en de ambtenaren van het secretariaat zijn vervolgens in artikel 61, eerste lid, van de Wbp aangewezen als bevoegde toezichthouder (feitelijke uitvoerder van het toezicht) in de zin van artikel 5:11 van de Awb, toegerust met toezichts- en handhavingsbevoegdheden op grond van artikel 61 van de Wbp en afdeling 5.2 van de Awb.<sup>567</sup>

### **Onderzoeksbevoegdheid van het CBP**

Artikel 60, eerste lid, van de Wbp bepaalt dat het CBP *“ambtshalve of op verzoek van een belanghebbende, een onderzoek [kan, toevoeging door het CBP] instellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.”*

Zoals hierboven onder het kopje ‘Toezichthoudende taak van het CBP’ vermeld, verwijst de term ‘bij en krachtens de wet’ in de Wbp in algemene zin naar wetten, algemene maatregelen van bestuur en andere regelingen op grond waarvan persoonsgegevens worden verwerkt, waaronder hoofdstuk 11 van de Tw.

Uit de wetsgeschiedenis bij artikel 60 van de Wbp blijkt dat ‘onderzoek instellen/doen’ een specifieke vorm (onderdeel) is van de taak ‘toezicht houden’: *“Het onderzoek en de weergave van de bevindingen vormt een onderdeel van de uitoefening van de toezichthoudende taak van de Registratiekamer en kan een voorbereiding zijn op nadere besluitvorming”*.<sup>568</sup>

Zoals hierboven onder het kopje ‘Toezichthoudende taak van het CBP’ vermeld, strekt de toezichthoudende taak van het CBP zich uit tot zowel het terrein van de Wbp als hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie.

Noch de tekst van de bepaling noch de wetsgeschiedenis biedt daarom steun voor de opvatting van Vodafone dat het CBP een wettelijke bevoegdheid ontbeert om

<sup>566</sup> Kamerstukken I 2003/04, 28 851, C, p. 34.

<sup>567</sup> Zie ook de wetsgeschiedenis bij artikel 61 van de Wbp: *“Het artikel [61 van de Wbp, toevoeging door het CBP] dient steeds in samenhang te worden gezien met Afdeling 5.2 Awb. In het eerste lid wordt geregeld welke personen zijn of kunnen worden belast met het toezicht op de naleving van hetgeen bij of krachtens dit wetsvoorstel is bepaald. Deze personen worden beschouwd als «toezichthouder» in de zin van artikel 5:11 Awb. Zij beschikken over de bevoegdheden van Afdeling 5.2 Awb.”* Kamerstukken II 1997/98, 25 892, nr. 3, p. 183.

<sup>568</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 183.

onderzoek te doen naar mogelijke overtreding van andere normen dan neergelegd in de Wbp.

Anders dan Vodafone betoogt, is het CBP op grond van artikel 60, eerste lid, van de Wbp bevoegd om een onderzoek in te stellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp en hoofdstuk 11 van de Tw.

### **Samenwerkingsafspraken van het CBP met respectievelijk de ACM en AT**

Naast het CBP zijn de ACM (tot 1 april 2013: OPTA) en Agentschap Telecom<sup>569</sup> op grond van artikel 15.1, eerste respectievelijk derde lid, van de Tw belast met het toezicht op de naleving van het bepaalde bij of krachtens bepalingen van de Tw, voor zover voor dit onderzoek van belang. Het CBP heeft in dat verband samenwerkingsafspraken met de ACM en Agentschap Telecom in de vorm van het Samenwerkingsprotocol CBP-OPTA respectievelijk de Samenwerkingsovereenkomst Agentschap Telecom-CBP (zijnde werkafspraken tussen de verschillende toezichthouders binnen de grenzen van de onderscheidene wetten waarin hun bevoegdheden zijn geregeld).<sup>570</sup>

Het Samenwerkingsprotocol CBP-OPTA regelt/geeft onder andere bepalingen over de behandeling bij samenlopende bevoegdheden en de uitwisseling en verstrekking van informatie tussen de ACM en het CBP (zie artikel 2 respectievelijk 10).

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.

Artikel 24 van de Wet OPTA regelde de verstrekking van gegevens of inlichtingen omtrent een onderneming door OPTA aan 'een instantie die op grond van bepalingen in andere wetten dan de Wet OPTA is belast met de uitvoering van toezichthoudende taken'. Artikel 24, derde lid, van de Wet OPTA bepaalde dat indien zo'n instantie gegevens of inlichtingen ontving van OPTA, deze instantie onderzocht of er in dat geval sprake is van een overtreding van de betreffende wettelijke regels. Op grond van artikel 10, derde lid, van het Samenwerkingsprotocol CBP-OPTA trad OPTA (daarom), in overleg met het CBP alvorens het CBP informatie te verstrekken op basis van artikel 24, tweede lid, van de Wet OPTA.

Artikel 1, tweede en derde lid, van de Samenwerkingsovereenkomst Agentschap Telecom-CBP bepaalt dat de onderzoeken naar de naleving van de bepalingen uit de Tw over het gebruik van verkeersgegevens worden uitgevoerd door Agentschap Telecom, tenzij het CBP in een ander kader dan (sec) naleving van de bepalingen uit de Tw over het gebruik van verkeersgegevens op (mogelijke) overtredingen van de Tw is gestuit. In dat laatste geval kan het CBP zelfstandig onderzoek verrichten.

---

<sup>569</sup> Zie artikel 2 van het Besluit aanwijzing toezichthouders Telecommunicatiewet.

<sup>570</sup> URL: [http://www.cbplib.nl/downloads\\_samenwerking/samenwerking\\_opta.pdf](http://www.cbplib.nl/downloads_samenwerking/samenwerking_opta.pdf) en [http://www.cbplib.nl/downloads\\_pb/pb\\_20090915\\_samenwerkingsovereenkomst\\_at\\_cbp.pdf](http://www.cbplib.nl/downloads_pb/pb_20090915_samenwerkingsovereenkomst_at_cbp.pdf) (URL's laatst bezocht op 29 mei 2013).

OPTA heeft onderzoek uitgevoerd onder KPN, Vodafone, T-Mobile en Tele2 naar de vraag of en zo ja, hoe zij hun dataverkeer analyseren. OPTA heeft haar onderzoeksmateriaal verstrekt aan het CBP op grond van artikel 10, eerste en derde lid, van het Samenwerkingsprotocol CBP-OPTA jo. artikel 24, tweede lid, van de Wet OPTA, tegen de achtergrond van de omstandigheid dat de onderzochte wetsartikelen uit de Tw nauw samenhangen met bepalingen in de Wbp (zwaartepunt in de toepassing van bepalingen van de Wbp). In haar voorlopige bevindingen heeft OPTA hierover opgemerkt: *“Het is voor het college [van de OPTA, toevoeging door het CBP] nog niet duidelijk of de inzet van de door de aanbieders gebruikte analysemiddelen en de daarbij verwerkte gegevens in alle gevallen gerechtvaardigd en proportioneel is in het licht van de zorgplicht van artikel 11.2 Tw. (...) Daarvoor is nader onderzoek nodig. Het is daarbij van belang dat artikel 11.2 Tw nauw samenhangt met het bepaalde in de Wet bescherming persoonsgegevens, waarop het CBP toeziet. Het CBP en het college hebben hierover overlegd. Op grond van het samenwerkingsprotocol is besloten dat het college zijn bevindingen en de onderzoeksgegevens naar de naleving van artikel 11.2 van de Tw ter beschikking stelt aan het CBP. Het CBP zal deze bevindingen en de onderzoeksgegevens betrekken bij zijn onderzoek naar de naleving van de Wbp en de verwerking van persoonsgegevens bij de inzet van DPI-technieken.”*<sup>571</sup> Het CBP is tijdens een onderzoek in dat kader op (mogelijke) overtredingen van de Tw gestuit.

Anders dan Vodafone betoogt, maken de samenwerkingsafspraken van het CBP met de ACM (tot 1 januari 2013: OPTA) en AT niet dat het onderzoek zou moeten worden uitgevoerd door die toezichthouders in plaats van het CBP (en evenmin dat Vodafone erop mocht vertrouwen dat dit zou gebeuren).

Door de informatieverstrekking door OPTA aan het CBP was/is het CBP niet langer (alleen) bevoegd, maar ook verplicht om ambtshalve een onderzoek in te stellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de Wbp en hoofdstuk 11 van de Tw (zie artikel 60, eerste lid, van de Wbp jo. artikel 24, derde lid, van de Wet OPTA).

Aangezien het CBP tijdens een onderzoek in een ander kader dan (sec) naleving van de bepalingen uit de Tw over het gebruik van verkeersgegevens op (mogelijke) overtredingen van de Tw is gestuit, kon het CBP op grond van artikel 1, derde lid, van de Samenwerkingsovereenkomst Agentschap Telecom-CBP op dit punt ook overigens zelfstandig onderzoek verrichten.

De zienswijze 2 van Vodafone heeft op het punt van de bevoegdheid van het CBP geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van Vodafone heeft op dit punt niet geleid tot aanpassing van de conclusies in het rapport.

---

<sup>571</sup> ‘Voorlopige bevindingen over gebruik Deep Packet Inspection Voorlopige bevindingen over gebruik Deep Packet Inspection’, *Onderzoek OPTA* 30 juni 2011.

### *Verwerking van persoonsgegevens*

**Zienswijze 2 Vodafone:** Vodafone betwist in haar zienswijze 2 dat alle door Vodafone middels data-analyse technieken verwerkte gegevens als persoonsgegevens kwalificeren. Vodafone wijst in dat verband op het volgende:

- (i) (onder verwijzing naar de wetsgeschiedenis bij de Wbp:) gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten alleen als persoonsgegevens worden beschouwd als die gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en daarvan is niet (altijd) sprake.<sup>572</sup> Het handhaven van de productvoorwaarden BloX, het faciliteren van het gebruik van gratis opwaardeersites door prepaid klanten, het verhelpen van verbindingproblemen in algemene zin, het optreden tegen spam, virussen en malware en het behandelen van klantklachten houden niet in dat Vodafone die gegevens verwerkt 'op een wijze die in het maatschappelijk verkeer de betrokkene raakt'.<sup>573</sup> Het gaat alleen om handelingen van Vodafone als aanbieder van communicatiediensten aan haar eigen klanten, in het kader van de optimalisering van de eigen dienstverlening; van enig breder effect van het verwerken van die gegevens in een maatschappelijke context, is geen sprake.<sup>574</sup>
- (ii) de tabel met het overzicht van verwerkte persoonsgegevens in het Conceptrapport definitieve bevindingen bevat fouten (Vodafone geeft in haar zienswijze 2 een beschrijving daarvan);<sup>575</sup>
- (iii) Vodafone betwist dat de genoemde gegevens, met uitzondering van MSISDN, IMSI en IMEI (de *identifying data*), persoonsgegevens zijn en merkt op dat het CBP ten onrechte geen onderscheid maakt tussen het IP-adres van een eindgebruiker en het IP-adres op netwerk-element niveau;<sup>576</sup>
- (iv) (onder verwijzing naar de wetsgeschiedenis bij de Wbp over de term 'persoonsgegevens:') benadrukt Vodafone dat ondenkbaar is dat zij de gegevens gebruikt voor direct marketing (en/of profilerings-)doeleinden;<sup>577</sup>
- (v) Vodafone betwist dat zij (in)direct identificerende gegevens, ter zake kundige technici en technische faciliteiten heeft om de gegevens te koppelen aan abonnees en dat daaruit blijkt dat de inspanning die Vodafone moet kunnen verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is;<sup>578</sup>
- (vi) omdat voor het doeleinde spam-, virus- en malwarebestrijding geen herleidbaarheid tot personen nodig is, aangezien spam-, virus- en malwarebestrijding plaatsvindt op core netwerkniveau en tot doel heeft bepaald verkeer tegen te houden zonder dat dit gevolgen heeft voor een eindgebruiker, dient de conclusie te zijn dat voor dit doeleinde geen persoonsgegevens worden verwerkt;<sup>579</sup>
- (vii) Vodafone meent dat het onbewezen is dat in de gevallen dat Vodafone niet beschikt over de NAW-gegevens van haar prepaid bellers die van

---

<sup>572</sup> Zienswijze 2 Vodafone, p. 41.

<sup>573</sup> Idem, p. 43.

<sup>574</sup> Idem, p. 43.

<sup>575</sup> Idem, p. 42.

<sup>576</sup> Idem, p. 42-43.

<sup>577</sup> Idem, p. 43.

<sup>578</sup> Idem, p. 44.

<sup>579</sup> Idem, p. 44.

datadiensten gebruik maken, zij wel de achterliggende persoon zou kunnen identificeren, al dan niet via tussenstappen. Ook begrijpt zij de verwijzing naar de arresten Scarlet/Sabam en Lindqvist van het Hof van Justitie niet;<sup>580</sup>

- (viii) Vodafone vindt de (deel)conclusie in het Conceptrapport definitieve bevindingen dat persoonsgegevens over het communicatiegedrag van betrokkenen gegevens van gevoelige aard zijn ontoereikend gemotiveerd. Het gaat niet om gegevens die wegens hun aard een inbreuk op fundamentele vrijheden kunnen maken.<sup>581</sup>

**Reactie CBP:** Voor zover Vodafone in haar zienswijze 2 (zie p. 168 van dit rapport, bullet points (ii) en (iii)) opmerkt dat de tabel met het overzicht van verwerkte persoonsgegevens in het Conceptrapport definitieve bevindingen fouten bevat, heeft de zienswijze 2 geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies.

### **Gegevens ‘betreffende’ een persoon**

Voor zover Vodafone zich in haar zienswijze 2 (zie p. 168 van dit rapport, bullet point (i)) op het standpunt stelt dat niet (altijd) sprake is van gegevens die medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, nu het in dit onderzoek alleen gaat om handelingen van Vodafone als aanbieder van communicatiediensten aan haar eigen klanten, wijst het CBP erop dat de term “maatschappelijk verkeer” in het normale taalgebruik (Van Dale Groot woordenboek van de Nederlandse taal) betekent omgang in de persoonlijke of zakelijke sfeer: het maatschappelijk verkeer tussen en met mensen als lid van het bestuurlijke, economische enz. leven, oftewel de manier waarop mensen in het dagelijkse leven met elkaar omgaan. Handelingen van Vodafone als aanbieder van communicatiediensten aan haar eigen klanten zijn onderdeel van het maatschappelijk verkeer.

Waar Vodafone benadrukt dat ondenkbaar is dat zij de gegevens voor direct marketing (en/of profilerings-)doeleinden gebruikt (zie p. 168 van dit rapport, bullet point (iv)), merkt het CBP op dat Vodafone in haar zienswijze 2 heeft volstaan met een loutere ontkenning, zonder concrete feiten aan te voeren ter weerlegging van de door het CBP onderbouwde stelling dat het mobiele data ge-/verbruik van een betrokkene een indicatie kan zijn voor bijvoorbeeld zijn interesses, sociale achtergrond, inkomen of gezinssamenstelling die kan worden gebruikt voor (direct) marketing- en profileringsdoeleinden.

### **Identificeerbaarheid van de persoon**

In die mate dat Vodafone in haar zienswijze 2 (zie p. 168 van dit rapport, bullet point (iii)) betwist dat de genoemde gegevens, met uitzondering van het MSISDN, IMSI en IMEI (de identificerende data), persoonsgegevens zijn, wijst het CBP op het volgende. Anders dan Vodafone meent, is niet zozeer doorslaggevend welke gegevens *identifiers* zijn, maar luidt het rechtens relevante criterium of de genoemde gegevens op zichzelf, in onderlinge combinatie of in samenhang met uit andere bron bekende informatie zonder onevenredige inspanning direct dan wel indirect herleidbaar zijn tot een

---

<sup>580</sup> Idem, p. 44 en 68.

<sup>581</sup> Idem, p. 45-46.

identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).<sup>582</sup> Aan dit criterium is voldaan.

De enkele betwisting door Vodafone (met in totaal 2.800 werknemers in Nederland<sup>583</sup>) dat zij (in)direct identificerende gegevens, ter zake kundige technici en technische faciliteiten heeft om de gegevens te koppelen aan abonnees en dat daaruit blijkt dat de inspanning die Vodafone moet kunnen verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is (zie p. 168 van dit rapport, bullet point (v)), is onvoldoende ter weerlegging van bijvoorbeeld het bewijs dat het CBP blijkens een screenshot gemaakt tijdens het onderzoek ter plaatse inzage heeft gehad in de ruwe data van de [VERTROUWELIJK: apparatuur], [VERTROUWELIJK]. NB Om te bepalen of een persoon identificeerbaar is, is het relevante criterium overigens of de gegevens zonder onevenredige inspanning direct of zo nodig via tussenstappen herleidbaar zijn tot een identificeerbare natuurlijke persoon *door de verantwoordelijke dan wel enig ander persoon* [VERTROUWELIJK].<sup>584</sup>

Voor zover Vodafone meent dat het onbewezen is dat in de gevallen dat Vodafone niet beschikt over de NAW-gegevens van haar prepaid bellers die van datadiensten gebruik maken, zij wel de achterliggende persoon zou kunnen identificeren (zie p. 169 van dit rapport, bullet point (viii)), benadrukt het CBP dat Vodafone echter wel beschikt over ten minste het MSISDN, IMSI- en IMEI-nummer, in combinatie met tijd. Nog daargelaten dat uit het Hof van Justitie-arrest Lindqvist en de opinie van de Artikel 29 Werkgroep over het begrip persoonsgegevens<sup>585</sup> volgt dat identificatie ook kan 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), is het MSISDN een direct contactgegeven door middel waarvan Vodafone met de abonnee in contact kan treden, om zijn identiteit vast te stellen. Vodafone heeft dit in haar zienswijze 2 onvoldoende weersproken. In het Hof van Justitie-arrest Scarlet/Sabam heeft het Hof van Justitie van de EU de gelegenheid gehad om te onderzoeken of en de vraag beantwoordt dat een IP-adres als zodanig als een persoonsgegeven is te beschouwen.<sup>586</sup>

Waar Vodafone betoogt dat voor het doeleinde spam-, virus- en malwarebestrijding geen herleidbaarheid tot personen nodig is en daarom de conclusie dient te zijn dat voor dit doeleinde geen persoonsgegevens worden verwerkt (zie p. 168 van dit rapport, bullet point (vi)), merkt het CBP op dat de vraag of *het doel* (oogmerk) van de gegevensverwerking identificeerbaarheid is niet hét criterium betreft ter bepaling van de vraag of sprake is van persoonsgegevens. Omgekeerd komt aanvoeren dat personen niet identificeerbaar zijn als het doel van de verwerking nu juist die identificatie is, wel neer op een contradictio in terminis.<sup>587</sup>

---

<sup>582</sup> Vgl. AbRvS 7 november 2012, LJN BY2508.

<sup>583</sup> [VERTROUWELIJK]

<sup>584</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48.

<sup>585</sup> HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27 en WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 14-15.

<sup>586</sup> Zie HvJ EU 24 november 2011, zaak C-70/10 (*Scarlet/Sabam*), r.o. 26 en AG HvJ 14 april 2011, zaak C-70/10, r.o. 74 tot en met 78.

<sup>587</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 45-50.

De betwisting van Vodafone dat persoonsgegevens over het communicatiegedrag van betrokkenen gegevens van gevoelige aard zijn omdat het niet gaat om gegevens die wegens hun aard een inbreuk op fundamentele vrijheden kunnen maken (zie p. 169 van dit rapport, bullet point (viii)), noopt niet tot een ander oordeel: uit deze verkeersgegevens volgt informatie over het communicatiegedrag van de betrokkene en soms ook over de inhoud van de communicatie. Dit raakt aldus het recht op vertrouwelijke communicatie.<sup>588</sup> Vodafone heeft dit onvoldoende weersproken.

De zienswijze 2 van Vodafone (zie p. 168 van dit rapport, bullet points (iii) en (viii)) heeft op het punt van de term “persoonsgegevens”, geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

#### *Verkeersgegevens versus communicatie*

**Zienswijze 2 Vodafone:** Vodafone betoogt in haar zienswijze 2 (nogmaals) dat een hostname/URL wordt omgezet om de transmissie tot stand te brengen. Een gebruiker toetst een URL in, die door de Domain Name Server (DNS) - technisch gezien - wordt vertaald naar het bijbehorende IP-adres. Vervolgens wordt de webserver benaderd die de webpagina herbergt. Hieruit volgt dat hostnames/URL's (ook) verkeersgegevens zijn (de steeds sterkere vervlechting van de gevoerde communicatie en de daarmee samenhangende gegevens en technische protocollen vormt juist een argument voor deze conclusie).<sup>589</sup> Dat deze gegevens niet onder de bewaarplicht van de Wet bewaarplicht telecommunicatiegegevens (geïmplementeerd in hoofdstuk 13 van de Tw) vallen, zegt niets over de vraag of het verkeersgegevens zijn.<sup>590</sup> Dat deze gegevens ‘gevoelige gegevens’ zouden zijn, of gegevens uit de inhoud van het dataverkeer of zowel verkeersgegevens als communicatie dan wel dat hieruit in elk geval informatie over de communicatie af te lezen is, is - net als de rest van deze paragraaf in het Conceptrapport definitieve bevindingen - ontoereikend gemotiveerd.<sup>591</sup> Vodafone betwist (daarnaast) dat voor zover ten aanzien van een toestel in stand-by stand (oftewel: idle mode) onder andere locatiegegevens worden verzonden over het signaleringskanaal om ervoor te zorgen dat het op elk moment inkomende berichten kan ontvangen, geldt dat geen sprake is van verkeersgegevens (alleen maar van persoonsgegevens) omdat er geen communicatie wordt/is gevoerd.<sup>592</sup> Volgens Vodafone is dit alles overigens niet relevant (juridisch noch feitelijk) voor dit onderzoek, nu het enige relevante criterium voor de bevoegdheid van het CBP is of sprake is van persoonsgegevens.<sup>593</sup> Verder merkt Vodafone in haar zienswijze 2 op dat het haar bevreemdt dat het CBP (louter) opmerkt dat Agentschap Telecom instemt met de invulling van de termen ‘communicatie’ en ‘verkeersgegevens’.<sup>594</sup> Dat

---

<sup>588</sup> 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](http://www.cbppweb.nl/Pages/adv_z2012-00746.aspx) (URL laatst bezocht op 29 mei 2013).

<sup>589</sup> Zienswijze 2 Vodafone, p. 47, 49 en 52-53.

<sup>590</sup> Idem, p. 49.

<sup>591</sup> Idem, p. 48, 50 en 52-53.

<sup>592</sup> Idem, p. 48.

<sup>593</sup> Idem, p. 46-49.

<sup>594</sup> Idem, p. 50.



app/protocol/service/herkenningsgegevens gegevens zijn die de inhoud van het dataverkeer raken, lijkt (ten slotte) gemeengoed in de literatuur over DPI, maar het zijn volgens Vodafone geen persoonsgegevens.<sup>595</sup>

**Reactie CBP:** Het CBP volgt Vodafone in haar betoog dat het toetsingskader voor de verwerking van URL's (waaronder mede begrepen hostnames) het regime voor verwerking van verkeersgegevens is (oftewel, volgens het CBP: artikel 11.5 van de Twjo. artikel 8 van de Wbp). De zienswijze 2 van Vodafone heeft op het punt van het toetsingskader voor de verwerking van URL's geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport.

Dit neemt niet weg dat omdat verkeersgegevens veel over de gebruiker kunnen zeggen en raken aan de telecommunicatievrijheid, verkeersgegevens die ook persoonsgegevens zijn ook wel worden aangeduid als gegevens van gevoelige aard.<sup>596</sup> Het CBP wijst er in dat verband verder op dat zowel de inhoud van, als 'informatie over elektronische communicatie' (oftewel, verkeersgegevens) gegevens zijn die bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (Handvest).<sup>597</sup>

*Overige opmerkingen wettelijk kader*

#### **Gegevensverwerking**

**Zienswijze 2 Vodafone:** Volgens Vodafone stoelt de beoordeling/conclusie in het Conceptrapport definitieve bevindingen dat sprake is van gegevensverwerking op ondeugdelijke feitelijke en juridische gevolgtrekkingen en is deze daarmee onjuist en onzorgvuldig.<sup>598</sup>

**Reactie CBP:** Het CBP heeft hierboven onder het kopje 'Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering' gemotiveerd dat het onderzoek zorgvuldig is voorbereid. Het onderzoek/dit naar aanleiding van de zienswijzen van Vodafone gedeeltelijk aangepaste rapport is ook toereikend gemotiveerd. De beoordeling/conclusie in het Conceptrapport definitieve bevindingen dat sprake is van gegevensverwerking berust daarom op een deugdelijke motivering. De zienswijze 2 van Vodafone heeft op het punt van de gegevensverwerking (desondanks) geleid tot een nadere toelichting van het toepasselijke en toegepaste wettelijk kader in het rapport.

De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van de conclusies in het rapport.

---

<sup>595</sup> Idem, p. 50 en 53.

<sup>596</sup> Vgl. *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. Zie ook idem, nr. 1, p. 27: "(...) het feit dat verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens (...)." Zie ook *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. Idem, nr. 1, p. 27.

<sup>597</sup> Zie o.a. EHRM 3 april 2007, NJ 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44; EHRM 2 augustus 1984, NJ 1988, 534 (Malone) en EHRM 25 september 2001, NJ 2003, 670 (P.G. en J.H./Verenigd Koninkrijk). Zie ook CBP wetgevingsadvies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet van 11 februari 2013.

<sup>598</sup> Zienswijze 2 Vodafone, p. 51.

### **Grondslag**

**Zienswijze 2 Vodafone:** Volgens Vodafone kunnen verwijzingen naar eerdere besluiten van het CBP dan wel verwijzingen naar standpunten van de Artikel 29-werkgroep weinig of geen gewicht toekomen (*oratio pro domo*).<sup>599</sup> Het Huber-arrest van het Hof van Justitie is niet relevant omdat dit arrest enkel iets zegt over de noodzakelijkheid van het verzamelen en bewaren van gegevens op naam door de Duitse overheid ten behoeve van een zogenaamd ‘Ausländerzentralregister’ omtrent in Duitsland verblijvende burgers van de Unie: een onvergelijkbaar geval, aldus Vodafone: het doel is niet vergaring van statistische gegevens, maar het mogelijk maken van de reguliere bedrijfsvoering van een provider.<sup>600</sup>

Vodafone bestrijdt dat verkeersgegevens moeten worden vernietigd wanneer de factuur (binnen de vervalltermijn) is voldaan. Betaling van de factuur binnen de vervalltermijn staat immers niet in de weg aan de betwisting ervan (binnen vijf jaar) door de klant.<sup>601</sup>

### **Artikel 29-werkgroep**

**Reactie CBP:** Voor zover Vodafone in haar zienswijze 2 betoogt dat standpunten van de Artikel 29-werkgroep, het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, weinig of geen gewicht toekomen, is van belang dat deze groep is ingesteld in artikel 29 van de Privacyrichtlijn. Ze is onafhankelijk en raadgevend van aard en heeft onder andere tot taak elke kwestie betreffende de toepassing van de ter uitvoering van deze richtlijn vastgestelde nationale bepalingen te bestuderen, *teneinde bij te dragen tot een homogene toepassing daarvan*. De Artikel 29-werkgroep publiceert in dat verband regelmatig werkdokument en opinies met uitleg over de toepassing van de Privacyrichtlijn, over voorstellen voor nieuwe wetgeving, en over overige onderwerpen die zich afspelen op het gebied van bescherming van persoonsgegevens. Gelet op de wettelijke taak komen aan standpunten van de Artikel 29-werkgroep reeds hierom gewicht toe.

Ten overvloede wijst het CBP er - in algemene zin - op dat een bestuursorgaan beleidsregels kan vaststellen omtrent de uitleg van wettelijke voorschriften bij het gebruik van zijn bevoegdheden, waaraan het bestuursorgaan in beginsel ook gebonden is (artikel 4:81 jo. 4:84 van de Awb).

### **Hof van Justitie-arrest Huber**

Waar Vodafone in haar zienswijze 2 de relevantie van het Hof van Justitie-arrest Huber betwist, benadrukt het CBP de betekenis hiervan. Ten eerste vanwege de overweging dat het begrip “noodzakelijkheid” een autonoom begrip van gemeenschapsrecht is en dus niet een inhoud kan hebben die verschilt van lidstaat tot lidstaat.<sup>602</sup> Ten tweede omdat uit het arrest de volgende algemene regel kan worden afgeleid: dat indien het doel de vergaring van statistische gegevens is, het niet noodzakelijk is de persoonsgegevens op naam te bewaren en te verwerken.<sup>603</sup>

---

<sup>599</sup> Idem.

<sup>600</sup> Idem, p. 51 en 54-55.

<sup>601</sup> Idem, p. 52.

<sup>602</sup> Vgl. ook HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 52.

<sup>603</sup> HvJ EG 16 december 2008, EHRC 2009, 23 (LJN BG7811; Huber), r.o. 64-65 en 68: “*Evenzo gaat verordening nr. 862/2007, die de verstrekking regelt van statistische gegevens over de migratiebewegingen op het grondgebied van de lidstaten, ervan uit dat de lidstaten de informatie*

Vodafone geeft onder andere in haar zienswijze 2 aan dat zij niet altijd op individueel klantniveau gegevens verwerkt om valide, bruikbare informatie te krijgen over de netwerkbelasting als gevolg van de toename van dataverkeer, maar dat zij trends moet kunnen onderkennen, bijvoorbeeld om op tijd knelpunten in het netwerk te herkennen, zodat ze eventueel de netwerkcapaciteit kan uitbreiden'.<sup>604</sup> Om zulke trends te berekenen is statistische analyse nodig.

#### Geen overtreding van privacyregels: overige opmerkingen en aanvullingen beoordeling

##### *Doeleinde verkeersbeheer*

**Zienswijze 2 Vodafone:** Vodafone betwijfelt de relevantie van de omstandigheid dat - volgens het CBP - gelet op de aard van de verzamelde persoonsgegevens en de omstandigheden waaronder ze worden verkregen, bovengemiddeld rekening moet worden gehouden met het risico op verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld.<sup>605</sup>

Vodafone concludeert (verder) dat de conclusie dat de verwerking niet kan worden gebaseerd op de grondslag uitvoering van een overeenkomst - dan wel gerechtvaardigd belang<sup>606</sup> - niet houdbaar is, nu zij heeft aangetoond dat deze grondslag uitvoering van een overeenkomst, voor zover daar nog aan toe wordt gekomen gezien de grondslag van artikel 11.5 van de Tw, bestaat, terwijl het CBP daar niet meer tegenover weet te stellen dan een ongemotiveerde, onbewezen stelling dat een lichtere maatregel mogelijk zou zijn.<sup>607</sup>

Vodafone handhaaft (daarnaast) al haar stellingen dat sprake is van een wettelijke plicht, omdat de weerlegging van het CBP volgens haar niet overtuigt.<sup>608</sup> In haar reactie op de vordering van het CBP voegt Vodafone er aan toe dat het haar is toegestaan om op (kern-)netwerkniveau het verkeer te kunnen afleveren data-analyse technieken toe te passen (zie ook de wettelijke uitzonderingsgrond in artikel 11.2a, tweede lid, onder c, van de Tw).

Vodafone bestrijdt dat de bewijslast ten aanzien van de proportionaliteit van de verwerking op haar rust.<sup>609</sup>

---

*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."*

<sup>604</sup> Zie o.a. Zienswijze 2 Vodafone, p. 26-27 en 30 en 56.

<sup>605</sup> Zienswijze 2 Vodafone, p. 59.

<sup>606</sup> Idem, p. 63.

<sup>607</sup> Idem, p. 61. Zie ook Reactie Vodafone op vordering van 21 februari 2013, p. 17.

<sup>608</sup> Zienswijze 2 Vodafone, p. 61.

<sup>609</sup> Idem, p. 62. Reactie Vodafone op vordering van 21 februari 2013, p. 3-4.

Vodafone brengt in haar zienswijze 2 (bovendien) naar voren dat het niet verstrekken van voldoende informatie geen belang is dat onder artikel 8, aanhef en onder f, kan worden meegewogen, ook omdat er op dit punt een zelfstandige verplichting op grond van de Wbp bestaat.<sup>610</sup>

Vodafone betwist de a contrario conclusie uit overwegingen 29 en 30 van de e-Privacyrichtlijn dat voor het meer algemene doel van verkeersbeheer, verwerking slechts in geaggregeerde vorm zou zijn toegelaten. Vodafone wijst erop dat er geen rechterlijke uitspraak is waaruit dit volgt en dat een richtlijnoverweging overigens ook geen bindend recht is.<sup>611</sup>

Vodafone bestrijdt dat het beginsel van dataminimalisatie, in het bijzonder zoals ingevuld met het beginsel van data siloing (persoonsgegevens die voor verschillende doeleinden worden verzameld, moeten gescheiden worden verwerkt) algemeen aanvaard is.<sup>612</sup>

### **Risico op verdere verwerking van de persoonsgegevens**

**Reactie CBP:** Voor zover Vodafone in haar zienswijze 2 de relevantie betwijfelt van de omstandigheid dat er gelet op de gevoelige aard van de verzamelde persoonsgegevens en de omstandigheden waaronder ze worden verkregen, rekening moet worden gehouden met een bovengemiddeld risico (qua impact) op verdere verwerking van de persoonsgegevens voor een ander doeleinde dan waarvoor ze oorspronkelijk zijn verzameld, wijst het CBP op het volgende.

Het bestuursorgaan dient de relevante belangen af te wegen (artikel 3:4 jo. 3:1 van de Awb).

In het kader van (de toets van) het verwerkingsdoel verkeersbeheer (artikel 11.5, eerste en/of tweede jo. vijfde lid, van de Tw) moet getoetst worden of deze verwerking voldoet aan het proportionaliteits- en subsidiariteitsvereiste. De aard van de verzamelde persoonsgegevens, de omstandigheden waaronder zij worden verkregen (te weten: het gebruik van automatische procedures voor 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 die belangenafweging. Evenals de kosten en tijd die voor Vodafone gepaard gaan met de ontwikkeling en implementatie van (technische) mogelijkheden om hetzelfde doel op een andere, minder inbreukmakende wijze te bereiken en de consequenties voor de continuïteit en integriteit van haar netwerk.

De zienswijze 2 van Vodafone heeft op het punt van het risico op verdere verwerking van de persoonsgegevens niet geleid tot aanpassing van de feitelijke bevindingen en conclusies in het rapport.

---

<sup>610</sup> Zienswijze 2 Vodafone, p. 62.

<sup>611</sup> Idem.

<sup>612</sup> Idem, p. 66.

### **Uitvoering van een overeenkomst en gerechtvaardigd belang**

Waar Vodafone in haar zienswijze 2 naar voren brengt dat de conclusie dat de verwerking niet kan worden gebaseerd op de grondslag uitvoering van een overeenkomst - dan wel gerechtvaardigd belang - niet houdbaar is, nu zij heeft aangetoond dat deze grondslag uitvoering van een overeenkomst, voor zover daar nog aan toe wordt gekomen gezien de grondslag van artikel 11.5 van de Tw, bestaat, verwijst het CBP naar de nadere toelichting van het toepasselijke en toegepaste wettelijk kader op het punt van de samenloop van Wbp en Tw waaruit (inderdaad) volgt 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.

De zienswijze 2 van Vodafone heeft op het punt van de noodzaak voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer (meer in het bijzonder: netwerkplanning respectievelijk netwerkmonitoring) via de [VERTROUWELIJK: apparatuur] en de [VERTROUWELIJK: apparatuur] (gedeeltelijk) geleid tot aanpassing van de conclusies in het rapport.

Vodafone heeft evenwel in haar zienswijze 2 voor het overige onvoldoende concrete feiten aangevoerd ter weerlegging van de door het CBP onderbouwde stelling dat er ten aanzien van bepaalde data-analyse technieken (in het kader van de 'subdoeleinden' netwerkplanning, netwerkmonitoring en het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites) alternatieve maatregelen kunnen worden gebruikt waarbij de verwerking van het aantal persoonsgegevens beperkter is (als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren).

### **Wettelijke plicht**

Voor zover Vodafone in haar zienswijze 2 haar stellingen handhaaft dat sprake is van een wettelijke plicht, heeft Vodafone dit standpunt in haar zienswijze 2 onvoldoende onderbouwd.

Waar Vodafone in haar reactie op de vordering van het CBP daaraan toevoegt dat het haar is toegestaan om op (kern-)netwerkniveau het verkeer te kunnen afleveren data-analyse technieken toe te passen (zie ook de wettelijke uitzonderingsgrond in artikel 11.2a, tweede lid, onder c, van de Tw, wijst het CBP erop dat dit artikel echter op zichzelf geen grondslag voor de verwerking van communicatie, tevens persoonsgegevens (maar uitzonderingen op het verwerkingsverbod) geeft (zie hierover verder het kopje 'Samenloop Wbp en Tw').

De zienswijze 2 van Vodafone heeft op het punt van de grondslag 'wettelijke plicht' niet geleid tot aanpassing van de conclusies in het rapport.

### **Bewijslast proportionaliteit van de verwerking**

Voor zover Vodafone in haar zienswijze 2 bestrijdt dat de bewijslast ten aanzien van de proportionaliteit van de verwerking op haar rust, geldt dat hoofdregel is dat bij het nemen van een belastende beschikking de bewijs(voerings)last (plicht tot kennisvergaring) in beginsel op het bestuursorgaan rust. Niettemin kan zich de

situatie voordoen dat bijvoorbeeld uit de parlementaire geschiedenis van een wetsartikel blijkt welke partij de bewijslast zou moeten dragen. De plicht om de noodzaak van de verwerking aan te tonen berust onder het Wbp-regime bij de verantwoordelijke.<sup>613</sup> Ook de volgende factoren (vuistregels) kunnen de verdeling van de bewijslast beïnvloeden: de partij die belang heeft bij een bepaald feit, draagt de bewijslast, de partij in wier bewijsdomein het feit ligt, draagt de bewijslast en de partij die zich op een uitzondering of een verandering beroept, draagt de bewijslast.<sup>614</sup> Het bestuursorgaan dient (verder) weliswaar de relevante belangen af te wegen (artikel 3:4 jo. 3:1 van de Awb). De belanghebbende draagt de bewijslast voor de stelling dat zijn belang onevenredig zwaar wordt getroffen (artikel 3:4 jo. artikel 3:1 van de Awb) (zie hierover verder het kopje 'Plicht tot een zorgvuldige kennisvergaring en belangenafweging en een toereikende motivering').

De zienswijze 2 van Vodafone heeft op het punt van de bewijslast van de proportionaliteit van de verwerking niet geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader en de conclusies in het rapport.

#### **Het niet verstrekken van voldoende informatie geen mee te wegen belang**

In die mate dat Vodafone in haar zienswijze 2 naar voren brengt dat het niet verstrekken van voldoende informatie geen belang is dat onder artikel 8, aanhef en onder f, van de Wbp kan worden meegewogen, merkt het CBP op dat er geen wettelijk voorschrift of algemeen rechtsbeginsel is dat meebrengt dat het ontbreken van toereikende informatie geen rol kan spelen bij de beantwoording van de vraag of de verantwoordelijke een juiste afweging van belangen heeft gemaakt.<sup>615</sup> Het uitgangspunt is welbeschouwd dat de belangen van de betrokkene in mindere mate gewicht in de schaal leggen naarmate in zijn belang meer waarborgen voor een zorgvuldig gebruik van de gegevens zijn genomen.<sup>616</sup>

De zienswijze 2 van Vodafone heeft op het punt van het niet verstrekken van voldoende informatie als mee te wegen belang niet geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader en de conclusies in het rapport.

#### **Overwegingen 29 en 30 van de e-Privacyrichtlijn**

Waar Vodafone zich verzet tegen de a contrario conclusie uit overwegingen 29 en 30 van de e-Privacyrichtlijn dat voor het meer algemene doel van verkeersbeheer, verwerking slechts in geaggregeerde vorm zou zijn toegelaten, merkt het CBP dat deze overwegingen (louter) onderstrepen dat het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het verwerkingsdoel verkeersbeheer alleen is

---

<sup>613</sup> Kamerstukken II 1998/99, 25 892, nr. 13, p. 6: "Overigens wijzen wij erop dat alleen een gerechtvaardigd belang niet voldoende is. Gegevensverwerking is blijkens artikel 8, onder f, alleen toelaatbaar indien deze met het oog op het desbetreffende belang ook «noodzakelijk» is. De plicht om de noodzaak van de verwerking aan te tonen berust bij de verantwoordelijke."

<sup>614</sup> Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. Amsterdam VU), Leiden: Kluwer 2005, p. 137-141.

<sup>615</sup> Vgl. Kamerstukken II 1997/98, 25 892, nr. 3, p. 91 over de verenigbaarheidstoets in artikel 9 van de Wbp: "Welke waarborgen passend zijn zal per concreet geval moeten worden beoordeeld. Het kan zijn dat de betrokkene over het voorgenomen gebruik wordt geïnformeerd, dan wel - een stap verder - in de gelegenheid wordt gesteld om zijn zienswijze hieromtrent te geven. De meest vergaande variant zou zijn indien aan de betrokkene voor het betreffende gebruik om toestemming wordt gevraagd."

<sup>616</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 88.

toegestaan als de persoonsgegevens zo snel als mogelijk na het verzamelen worden verwijderd, bijvoorbeeld door deze te anonimiseren.

De zienswijze 2 van Vodafone heeft op dit punt geleid tot verduidelijking van het toepasselijke en toegepaste wettelijk kader en de conclusies in het rapport.

### **Het beginsel van dataminimalisatie/data siloing**

Voor zover Vodafone in haar zienswijze 2 bestrijdt dat persoonsgegevens die voor verschillende doeleinden worden verzameld, gescheiden moeten worden verwerkt, geldt het volgende.

Het beginsel van dataminimalisatie/data siloing volgt uit onder andere uit de OECD Privacy Principles (*Collection Limitation Principle*),<sup>617</sup> het Dataprotectieverdrag van de Raad van Europa uit 1981 (*personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*),<sup>618</sup> de Resolutie van het Europees Parlement van 6 juli 2011 over een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie,<sup>619</sup> (de toelichting bij) het Voorstel voor een algemene verordening gegevensbescherming<sup>620</sup> en de opinie van de Artikel 29-werkgroep over doelbinding (*'data silo'-ing, to ensure functional separation*).<sup>621</sup>

De zienswijze 2 van Vodafone heeft op het punt van het beginsel van dataminimalisatie/data siloing (wel) ertoe geleid dat is aangevuld en verduidelijkt dat het CBP in het rapport daarmee als zodanig (nog) niet het gebruik van een specifiek(e) product of techniek voorschrijft. De zienswijze 2 van Vodafone heeft op dit punt voor het overige niet geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader en de conclusies in het rapport.

### **'Subdoeleinde' video-optimalisatie en doeleinde beveiliging (spam- en virusfiltering en malwarebestrijding)**

**Zienswijze 2 Vodafone:** de opmerking in het Conceptrapport definitieve bevindingen dat de conclusie dat het CBP ter zake van de grondslag op deze punten geen overtreding constateert de informatieplicht van Vodafone onverlet laat, dient volgens Vodafone geen redelijk doel en moet worden verwijderd.<sup>622</sup>

**Reactie CBP:** Nu de informatieplicht rechtstreeks uit de wet volgt en Vodafone een professionele marktdeelnemer is, heeft het CBP deze overweging ten overvloede dat de conclusie dat het CBP ter zake van de grondslag geen overtreding constateert de

---

<sup>617</sup> URL:

<http://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm> (URL laatst bezocht op 29 mei 2013).

<sup>618</sup> URL: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (URL laatst bezocht op 29 mei 2013).

<sup>619</sup> URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:033E:0101:0110:NL:PDF> (URL laatst bezocht op 29 mei 2013).

<sup>620</sup> URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:HTML> (URL laatst bezocht op 29 mei 2013).

<sup>621</sup> WP29 203. Opinion 03/2013 on purpose limitation van 2 april 2013, p. 31.

<sup>622</sup> Zienswijze 2 Vodafone, p. 67.

informatieplicht van Vodafone onverlet laat, in dit rapport verwijderd. De zienswijze 2 van Vodafone heeft op dit punt geleid tot aanpassing van het rapport.

### *Doeleinde behandeling van verzoeken om inlichtingen van klanten*

**Zienswijze 2 Vodafone:** Vodafone betwist dat toestemming de enige mogelijke grondslag is voor dit doeleinde behandeling van verzoeken om inlichtingen van klanten, naast (ook) een gerechtvaardigd belang.<sup>623</sup>

Voor zover het CBP concludeert dat de toestemming niet 'voorafgaand' is, omdat deze pas wordt gevraagd op het moment dat de abonnee belt met een vraag of een klacht (medewerkers kunnen immers tot vijf dagen terug in de tijd kijken naar onder meer het datagebruik), wijst Vodafone erop dat zij hierdoor juist een effectievere waarborg inbrengt. Klanten worden hierdoor op het precieze moment dat dit er toe doet, gevraagd om toestemming te geven, en niet in abstracto vooraf. Vodafone voegt daar onder andere aan toe dat in het Privacy Statement al wel wordt geïnformeerd dat Vodafone op dat moment om toestemming zal vragen. Vodafone meent dat het CBP het toestemmingsvereiste teleologisch dient te interpreteren, althans dat zij met deze zorgvuldige handelswijze in elk geval een gerechtvaardigd belang heeft.<sup>624</sup>

**Reactie CBP:** Op grond van artikel 11.5, vijfde jo. eerste en/of tweede lid, van de Tw mogen persoonsgegevens die ook verkeersgegevens zijn (ook) voor de behandeling van verzoeken om inlichtingen van abonnees worden verwerkt, voor zover noodzakelijk. De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het doeleinde behandeling van verzoeken om inlichtingen van klanten geleid tot aanpassing van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies dat het CBP ten aanzien van deze gegevensverwerking geen overtreding heeft geconstateerd van de wet.

Voor zover Vodafone voor het doeleinde behandeling van verzoeken om inlichtingen van klanten ook persoonsgegevens die ook communicatie betreffen verwerkt, 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. Als een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zulke gegevens wil gebruiken voor de genoemde (uitgezonderde) doelen, dan zal hij de gegevensverwerking nog wel moeten kunnen baseren op een van de grondslagen als opgesomd in artikel 8 van de Wbp. 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. Vodafone heeft verklaard dat de verwerking van

---

<sup>623</sup> Idem.

<sup>624</sup> Idem, p. 67-68.



persoonsgegevens in individuele gevallen is gebaseerd op toestemming.<sup>625</sup> Van een geldige grondslag is (echter) slechts sprake indien deze toestemming ‘voorafgaand’ is.<sup>626</sup> Vodafone kan op dit punt een wettelijke grondslag voor de verwerking ten behoeve van behandeling van verzoeken om inlichtingen van klanten hebben, mits Vodafone betrokkenen om voorafgaande ondubbelzinnige toestemming zou vragen (dat wil zeggen: voorafgaand aan de gegevensverzameling) en die toestemming wordt verkregen. Dit is evenwel niet door het CBP onderzocht.

De zienswijze 2 van Vodafone heeft op dit punt geleid tot aanpassing en verduidelijking van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies dat het CBP.

***‘Subdoeleinde’ het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites***

**Zienswijze 2 Vodafone:** Vodafone wijst erop dat het hier niet gaat om een zelfstandig doeleinde maar om een onderdeel van het bredere doel ‘facturering’ en dat het daarmee valt onder artikel 11.5 van de Tw (voor zover sprake is van verkeersgegevensverwerking). Daarnaast geldt als grondslag de ‘uitvoering van een overeenkomst’.<sup>627</sup>

Vodafone licht in haar zienswijze 2 toe dat de overeenkomst tussen haar en een eindgebruiker tot stand komt door ingebruikname van een prepaid sim-kaart en eindigt door een afsluiting van deze sim-kaart van het netwerk (artikel 4, eerste lid, van de Algemene Voorwaarden voor Consumenten). De overeenkomst eindigt niet als zijn tegoed op is. Surfen naar de opwaardeersite vindt plaats in een contractuele context: Vodafone biedt de mogelijkheid tot gratis opwaardering (aanbod) en zodra de gratis site wordt bezocht, wordt dat aanbod (dat wil zeggen: de mogelijkheid om gratis op te waarderen) aanvaard.<sup>628</sup>

Vodafone merkt op dat niet door het CBP is gesteld en ook geen onderdeel van het onderzoek is geweest dat ook gegevens zouden worden verwerkt van abonnees met een toereikend tegoed.<sup>629</sup>

Vodafone betwist ook dat het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites bij een ontoereikend prepaid tegoed naar zijn aard een verkoopactiviteit is waarvoor toestemming is vereist, nu dit valt onder een en hetzelfde contract dan wel het aanvaarding is van het aanbod om zonder meerkosten voor datagebruik het tegoed op te waarderen. Los daarvan is het volgens Vodafone zo

---

<sup>625</sup> Zie Reactie Vodafone op verzoek om inlichtingen OPTA van 24 mei 2011, p. 2.

<sup>626</sup> Vgl. *Kamerstukken II* 1998/99, 25 892, nr. 9, p. 5 en URL: [http://www.cbpreweb.nl/pages/med\\_20120514\\_televisieopnamen-vumc-strijdig-met-wbp.aspx](http://www.cbpreweb.nl/pages/med_20120514_televisieopnamen-vumc-strijdig-met-wbp.aspx) (URL laatst bezocht op 29 mei 2013). Zie ook WP29 187, Advies 15/2011 over de definitie van “toestemming” van 13 juli 2011, p. 35-36 en 40: “Het is verstandig om toestemming te verkrijgen voordat met de gegevensverwerking wordt begonnen. Als dat niet gebeurt, is het gedeelte van de verwerking dat heeft plaatsgevonden tussen de start van de verwerking en het moment dat de toestemming wordt verkregen onrechtmatig, omdat er geen wettelijke grond voor bestaat.”

<sup>627</sup> Zienswijze 2 Vodafone, p. 68.

<sup>628</sup> Idem, p. 68-69.

<sup>629</sup> Idem, p. 69.

dat als deze redenering zou worden doorgetrokken zij steeds als de abonnee surft naar een site waar hij iets kan kopen, Vodafone dat alleen kan faciliteren als daarvoor toestemming wordt gegeven.<sup>630</sup>

**Reactie CBP:** Volgens Van Dale betekent de term “factureren” een factuur of facturen opmaken (van -) of op een factuur vermelden. Uit de wetsgeschiedenis bij de Tw volgt (inderdaad) dat het verwerkingsdoel facturering, genoemd in artikel 11.5, tweede lid, van de Tw, ‘ruim’ dient te worden opgevat in de zin dat verkeersgegevens ook mogen worden verwerkt van prepaid klanten die geen factuur ontvangen, maar waarbij de verwerking van die gegevens wel noodzakelijk is in verband met het registreren van hun beltegoed (dit laatste dient onder facturering te worden begrepen).<sup>631</sup> Dit verwerkingsdoel correspondeert met de grondslag uitvoering van een overeenkomst en - mogelijk - noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke, voor zover het belang van de betrokkenen niet prevaleert (artikel 8, aanhef en onder b en/of f, van de Wbp).

De enkele omstandigheid dat onder de verwerking ten behoeve van de facturering niet alleen wordt verstaan het opstellen van een factuur, maar ook het afwaarderen van het prepaidtegoed bij gebruik van de prepaidaansluiting met de verschuldigde vergoedingen en het bijhouden van het tegoed (het betreft immers vooruitbetaald(e) kaarten/gebruiksrechten, als het prepaidtegoed ontoereikend is om de verschuldigde vergoedingen te voldoen, is het niet mogelijk de relevante dienst (nog) te gebruiken), maakt niet dat het bieden van de mogelijkheid om nieuw tegoed te kopen daar ook zonder meer onder valt. Het faciliteren van opwaardeermogelijkheden is in beginsel - naar zijn aard - veeleer een verkoopactiviteit in de zin van artikel 11.5, derde lid, van de Tw waarvoor toestemming is vereist (die bij opwaardering een betalingsverplichting in het leven roept wat (wederom) noodzaakt tot het bijhouden van het tegoed). Volgens Van Dale betekent de term “verkopen” voor geld, tegen een bepaalde prijs, aan een ander overdoen, vooral om winst te maken, als beroep.

Op grond van haar algemene voorwaarden ‘Algemene Voorwaarden Consumenten Vodafone Libertel B.V.’ wordt de prepaid-overeenkomst in principe gesloten voor onbepaalde duur: *“Is jouw tegoed verbruikt of verlopen, dan kun je nog maar beperkt gebruik maken van jouw prepaid-overeenkomst (zoals bijvoorbeeld bellen naar 112). Binnen een bepaalde termijn kun je nieuw tegoed kopen”*, (artikel 4, eerste lid). Het CBP volgt Vodafone in haar betoog dat surfen naar de opwaardeersite aldus plaatsvindt in een contractuele context, dan wel het aanvaarding is van het aanbod van Vodafone om zonder meerkosten voor datagebruik het tegoed (ook) via ‘mobiel internet’ op te kunnen waarderen (om te voorkomen dat de betrokken abonnee zijn prepaid tegoed alsdan alleen kan opwaarderen via bijvoorbeeld een andere, ‘vaste’ internetverbinding). Dit ook vanuit de grondgedachte dat een eindgebruiker binnen een bepaalde termijn nieuw tegoed moet kunnen kopen. Hieruit volgt dat de verwerking van gegevens om opwaardeermogelijkheden te bieden noodzakelijk kan zijn voor de facturering. Een abonnee verwacht dit ook.

Het CBP heeft deze uitleg van de wet, dat het faciliteren van opwaardeermogelijkheden op het eerste gezicht wellicht een verkoopactiviteit lijkt

---

<sup>630</sup> Idem, p. 70.

<sup>631</sup> *Kamerstukken II 2002/03, 28 851, nr. 13, p. 20.*

waarvoor toestemming is vereist, maar gelet op de contractuele context en vanuit de grondgedachte dat een eindgebruiker binnen een bepaalde termijn nieuw tegood moet kunnen kopen noodzakelijk kan zijn voor het ruime verwerkingsdoel facturering, (nogmaals) voorgelegd aan Agentschap Telecom in het kader van de Samenwerkingsovereenkomst Agentschap Telecom-CBP. Agentschap Telecom stemt in met deze voorgelegde toepassing van dit wetsartikel.

De zienswijze 2 van Vodafone heeft op het punt van het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites geleid tot aanpassing van het toepasselijke en toegepaste wettelijk kader, evenals daarmee samenhangende wijziging(en) in de conclusies in het rapport dat het CBP ten aanzien van deze gegevensverwerking niet langer een overtreding heeft geconstateerd van de wet.

#### *Doeleinde verdere verwerking*

**Zienswijze 2 Vodafone:** Vodafone betwist dat de initiële verwerking in de [VERTROUWELIJK: apparatuur] onrechtmatig is en ook dat de verdere verwerking dat zou zijn. Los daarvan kan van een dubbele overtreding hoe dan ook geen sprake zijn: of Vodafone anonimiseert meteen en dan mag zij ook verder verwerken, of Vodafone laat die anonimisering te laat plaatsvinden (en dat is dan de verdere verwerking).<sup>632</sup>

**Reactie CBP:** Het CBP volgt Vodafone in haar betoog dat Vodafone een wettelijke grondslag heeft voor de verwerking ten behoeve van verkeersbeheer (meer in het bijzonder: netwerkplanning) via de [VERTROUWELIJK: apparatuur]. De zienswijze 2 van Vodafone heeft op dit punt geleid tot aanpassing en verduidelijking van de feitelijke bevindingen in het rapport, evenals daarmee samenhangende wijziging(en) in de conclusies dat het CBP (daarom) ten aanzien van deze verdere gegevensverwerking ook geen overtreding heeft geconstateerd van de wet.

#### *Uitdrukkelijk omschreven en gerechtvaardigde doeleinden*

**Zienswijze 2 Vodafone:** Vodafone blijft bij haar oordeel dat zij persoonsgegevens - voor zover sprake is van persoonsgegevens - voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verwerkt, en dat haar Privacy Statement daarvoor een 'uitdrukkelijke omschrijving' geeft, zodat geen sprake is van een schending van artikel 7 van de Wbp.<sup>633</sup>

**Reactie CBP:** Waar Vodafone aangeeft dat zij bij haar oordeel blijft dat zij persoonsgegevens - voor zover daarvan sprake is - voor gerechtvaardigde doeleinden verwerkt, merkt het CBP op dat Vodafone in haar zienswijze 2 heeft volstaan met een loutere stelling, zonder concrete feiten aan te voeren ter weerlegging van de door het CBP onderbouwde stelling dat de gegevensverwerking voor het doeleinde verkeersbeheer niet in alle stadia kan steunen op een of meer van de in artikel 8 van de Wbp genoemde gronden.

De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het doeleinde verkeersbeheer (meer in het bijzonder: netwerkplanning respectievelijk

---

<sup>632</sup> Zienswijze 2 Vodafone, p. 70.

<sup>633</sup> Idem, p. 71.

netwerkmonitoring) via de [VERTROUWELIJK: apparatuur] en de [VERTROUWELIJK: apparatuur] echter (gedeeltelijk) geleid tot aanpassing van de conclusies in het rapport. De zienswijze 2 van Vodafone heeft op het punt van de grondslag voor het verwerken van persoonsgegevens die ook verkeersgegevens zijn voor het 'subdoeleinde' het transporteren van het verkeer van prepaidklanten naar (gratis) opwaardeersites geleid tot aanpassing van de conclusies in het rapport dat het CBP ten aanzien van deze gegevensverwerking niet langer een overtreding heeft geconstateerd van de wet. De zienswijze 2 van Vodafone heeft daardoor eveneens geleid tot (gedeeltelijke) aanpassing van de conclusies in het rapport ten aanzien van het element 'gerechtvaardigde doeleinden'.

Ten aanzien van de stelling van Vodafone dat haar privacyverklaring een uitdrukkelijke omschrijving geeft van de doeleinden waarvoor zij persoonsgegevens verwerkt, neemt het CBP in aanmerking dat ofschoon blijkens de wetsgeschiedenis bij de vorm van de doelomschrijving lijkt te zijn gedacht aan de melding die zij op grond van artikel 27 jo. 28 van de Wbp (meldingsplicht) verplicht is te doen<sup>634</sup>, de recente opinie van de Artikel 29-werkgroep over doelbinding ook ruimte laat voor de vorm van verwoording en uitdrukking van de doeleinden in een privacystatement ('notice'): *"Expressing the purposes under the meaning of Article 6(1)(b) may be accomplished in different ways. These include, for example, describing the purposes in a notice provided to the data subjects, in a notification provided to the supervisory authority, or internally in the information provided to a data protection officer. Some national laws specifically provide that both notices and notifications are acceptable forms of complying with the requirement of making the purposes of the processing explicit, but that they are not the only possibilities",* (onderstreping toegevoegd door het CBP).<sup>635</sup>

De zienswijze 2 van Vodafone heeft op het punt van het toetsingskader voor de doelomschrijving geleid tot aanpassing en verduidelijking van het toepasselijke en toegepaste wettelijk kader. De zienswijze 2 van Vodafone heeft eveneens geleid tot aanpassing van de conclusies in het rapport ten aanzien van het element 'uitdrukkelijk omschreven'. De zienswijze 2 van Vodafone heeft voor het overige niet geleid tot aanpassing van de conclusies in het rapport.

---

<sup>634</sup> Zie Kamerstukken II 1997/98, 25 892, nr. 3, p. 20 en 79: "De omschrijving van het doel zal hetzij blijken uit de melding van de verwerking die de verantwoordelijke op grond van de wet uit hoofde van de wet verplicht is te verrichten - zie artikel 28, eerste lid, onder b, van het wetsvoorstel - hetzij uit de algemene maatregel van bestuur waarin precies zal worden geregeld welke verwerkingen van de meldingsverplichting worden vrijgesteld" en "Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen."

<sup>635</sup> WP29 203. Opinion 03/2013 on purpose limitation, dated 2 April 2013, p. 18.