

## **College bescherming persoonsgegevens**

Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door WhatsApp Inc.

Z2011-00987

Rapport definitieve bevindingen

Januari 2013

**OPENBARE VERSIE**

## INHOUDSOPGAVE

<b>Samenvatting .....</b>	<b>2</b>
<b>1. Inleiding.....</b>	<b>5</b>
<b>2. Bevindingen .....</b>	<b>9</b>
2.1 Whatsapp installeren en gebruiken .....	9
2.2 Toegang tot het adresboek op de smartphone .....	11
2.3 Bewaartermijnen gegevens van whatsapp-gebruikers .....	15
2.4 Beveiliging .....	16
2.4.1 Automatisch genereren van het wachtwoord.....	16
2.4.2 Beveiliging van de gegevensoverdracht via internet.....	17
2.5 Statusberichten.....	18
<b>3 Uitwerking van het wettelijk kader en beoordeling.....</b>	<b>20</b>
3.1 Toepasselijk recht .....	20
3.2 Bevoegdheid CBP .....	22
3.3 Verantwoordelijke .....	22
3.4 Vertegenwoordiger in Nederland .....	23
3.5 Verwerking van persoonsgegevens .....	23
3.6 Grondslag .....	29
3.6.1 Verwerking van gegevens van niet-gebruikers uit het adresboek van whatsapp-gebruikers.....	29
3.6.2 Statusberichten.....	33
3.7 Bovenmatigheid: toegang tot het adresboek op de smartphone .....	34
3.8 Bewaartermijn gegevens van whatsapp-gebruikers.....	35
3.9 Beveiliging .....	36
<b>4. Conclusies.....</b>	<b>40</b>

## SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft samen met de Canadese toezichthouder Office of the Privacy Commissioner of Canada (hierna: OPC) onderzoek ingesteld naar de verwerking van persoonsgegevens door WhatsApp Inc. (hierna: WhatsApp), ontwikkelaar van de mobiele communicatie-applicatie (app) whatsapp.

WhatsApp is gevestigd in Californië, de Verenigde Staten. De whatsapp-app is een veel gebruikte instant messaging app voor smartphones. De app is ontworpen als gratis internet alternatief voor SMS. De app is beschikbaar voor verschillende smartphones en besturingssystemen, waaronder de iPhone van Apple, de Windows Phone van Microsoft, de Blackberry van Research in Motion, de Nokia Symbian en S40 en apparaten met het Android besturingssysteem van Google. Met whatsapp kunnen gebruikers ook foto's, video's en geluidsbestanden verzenden en ontvangen (MMS).

Aanschaf van whatsapp voor de iPhone kost eenmalig 0,89 eurocent. Op andere besturingssystemen is de app gedurende het eerste jaar gratis. Het verzenden en ontvangen van berichten via de app is gratis. Gebruikers betalen alleen de kosten voor het datagebruik via internet.

De app is wereldwijd populair en staat in de top vijf van best verkopende apps. Volgens WhatsApp worden er sinds oktober 2011 via de app meer dan een miljard berichten per dag verstuurd.

Whatsapp is ook in Nederland een van de meest populaire apps, met miljoenen Nederlandse gebruikers. De app is zo bekend dat het werkwoord 'whatsappen' sinds oktober 2012 aan de Van Dale is toegevoegd.

### **Toepasselijk recht en bevoegdheid**

Het CBP is bevoegd om onderzoek in stellen op grond van de Wbp omdat via de app op smartphones in Nederland persoonsgegevens worden verwerkt. Het gaat onder meer om het mobiele telefoonnummer, unieke klant- en apparaatidentifiers en (als opgegeven) het push ID en de profielnaam van whatsapp-gebruikers. Daarnaast verwerkt WhatsApp het mobiele telefoonnummer van niet-gebruikers wanneer dat is opgenomen in het adresboek van whatsapp-gebruikers. WhatsApp gebruikt smartphones van whatsapp-gebruikers - door middel van de app die op de apparaten is geïnstalleerd - als middel bij de verwerking van persoonsgegevens in het kader van de app.

De Wet bescherming persoonsgegevens (Wbp) is (evenals hoofdstuk 11 van de Telecommunicatiewet; Tw) dwingend recht. Dit betekent dat de toepasselijkheid in deze kwestie daarvan niet via een eenzijdige verklaring of contractueel in de algemene voorwaarden door WhatsApp kan worden uitgesloten.

### **Toegang tot het adresboek**

Wie whatsapp wil gebruiken, moet toegang geven tot zijn volledige elektronische adresboek, inclusief de mobiele telefoonnummers van contacten die de app niet

**Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: (...)]

2

15 januari 2013

gebruiken (behalve in de laatste app versie op een iPhone met iOS 6). Doordat WhatsApp geen ondubbelzinnige toestemming verkrijgt van niet-gebruikers voor de verwerking van hun persoonsgegevens, en WhatsApp ook geen andere grondslag heeft voor deze gegevensverwerking, handelt WhatsApp in strijd met artikel 8 van de Wbp.

Om gebruikers in staat te stellen met elkaar te whatsappen, hoeft WhatsApp niet alle mobiele telefoonnummers uit hun adresboek te verwerken. Doordat WhatsApp gebruikers (behalve in de laatste app versie op een iPhone met iOS 6) niet de mogelijkheid biedt om te kiezen of zij hun contacten aan WhatsApp ter beschikking willen stellen en zo ja, welke, is een groot deel van de uit het adresboek verzamelde mobiele telefoonnummers bovenmatig. Hierdoor handelt WhatsApp in strijd met artikel 11, eerste lid, van de Wbp.

### **Bewaartermijn**

Van inactieve gebruikers bewaart WhatsApp nog gedurende een jaar persoonsgegevens. Doordat WhatsApp niet heeft aangetoond dat de gegevens van inactieve gebruikers zo lang bewaard moeten blijven, handelt WhatsApp in strijd met artikel 10, eerste lid, van de Wbp.

### **Beveiliging**

Bij aanvang van het onderzoek hebben het CBP en de OPC twee tekortkomingen in de beveiliging geconstateerd, ten aanzien van het aanmaken van wachtwoorden en ten aanzien van de verzending van berichten.

Bij aanvang van het onderzoek genereerde WhatsApp wachtwoorden door gebruik te maken van het gehashte WiFi MAC-adres op iPhones, en van het gehashte IMEI-toestelnummer op andere typen smartphones. Deze werkwijze stelde whatsapp-gebruikers bloot aan het risico dat anderen hun wachtwoord konden namaken, en daarmee namens hen berichten konden versturen en lezen. Hierdoor handelde WhatsApp in strijd met artikel 13 van de Wbp. Naar aanleiding van het rapport Voorlopige Bevindingen heeft WhatsApp haar werkwijze aangepast, en een nieuwe methode gekozen om wachtwoorden aan te maken. WhatsApp heeft in december 2012 updates van de app uitgebracht, en bij actieve gebruikers ervoor gezorgd dat zij gebruik (gaan) maken van de nieuwste versies door een geforceerde update. WhatsApp heeft aangegeven nog maatregelen te zullen treffen voor inactieve gebruikers. Doordat op dit moment WhatsApp nog niet voor alle accounts gebruik maakt van de nieuwe methode, handelt WhatsApp ten aanzien van deze gebruikers (nog) in strijd met artikel 13 van de Wbp.

Bij aanvang van het onderzoek door het CBP en de OPC verstuurde WhatsApp de berichten via de app op onversleutelde wijze. Hierdoor konden anderen de inhoud daarvan in leesbare vorm onderscheppen. Naar aanleiding van het onderzoek heeft WhatsApp versleuteling aangebracht. Hierdoor is de overtreding van artikel 13 van de Wbp op dit punt beëindigd.

### **Statusberichten**

Iedere whatsapp-gebruiker kan de statusberichten lezen van andere whatsapp-gebruikers, ook van onbekenden van wie hij de mobiele telefoonnummers in zijn adresboek heeft. Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp de informatie over de verspreiding van statusberichten aan haar gebruikers uitgebreid. De OPC benadrukt dat WhatsApp extra waarborgen moet inbouwen tegen de risico's van de brede verspreiding van potentieel gevoelige statusinformatie. Hoewel op dit punt formeel de Wbp niet lijkt te worden overtreden, onderschrijft het CBP de aanbeveling van de OPC dat gebruikers van WhatsApp een waarschuwing moeten krijgen, telkens als zij hun statusbericht aanpassen, over de verspreiding daarvan.

### **Aangekondigde maatregelen**

Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp aangekondigd dat (i) het adresseren van de wachtwoordbeveiliging van inactieve gebruikers, (ii) bewaartermijnen en de informatie daarover en (iii) het toevoegen van een waarschuwing/pop-up over de verspreiding van statusberichten - als gebruikers hun statusbericht aanpassen - op de agenda voor productontwikkeling staan. Whatsapp heeft daarbij geen termijnen genoemd.

## 1. INLEIDING

Het College bescherming persoonsgegevens (CBP) heeft samen met de Canadese toezichthouder Office of the Privacy Commissioner of Canada (hierna: OPC) onderzoek ingesteld naar de verwerking van persoonsgegevens door WhatsApp Inc. (hierna: WhatsApp), ontwikkelaar van de mobiele communicatie-applicatie (app) whatsapp.<sup>1</sup>

WhatsApp is opgericht in 2009 en gevestigd in Californië, de Verenigde Staten.<sup>2</sup> WhatsApp is de eigenaar en verantwoordelijke voor de website [www.whatsapp.com](http://www.whatsapp.com), de whatsapp software en de whatsapp-app.<sup>3</sup> WhatsApp heeft verklaard geen kantoren te hebben buiten de VS. WhatsApp heeft geen vertegenwoordiger aangewezen in Nederland.<sup>4</sup>

De whatsapp-app is een veelgebruikte instant messaging app voor smartphones. De app is ontworpen als gratis alternatief voor SMS. De app is beschikbaar voor verschillende smartphones en besturingssystemen, waaronder de iPhone van Apple, de Windows Phone van Microsoft, de Blackberry van Research in Motion, de Nokia Symbian en S40 en apparaten met het Android besturingssysteem van Google. Met whatsapp kunnen gebruikers ook foto's, video's en geluidsbestanden verzenden en ontvangen (MMS).

Aanschaf van whatsapp voor de iPhone kost eenmalig 0,89<sup>5</sup> (bij aanvang van het onderzoek: 0,79) eurocent. Op andere besturingssystemen is de app gedurende het eerste jaar gratis.<sup>6</sup> Het verzenden en ontvangen van berichten via de app is gratis. Gebruikers betalen alleen de kosten voor het datagebruik via internet.

De app is wereldwijd populair en staat in de top vijf van best verkopende apps. Volgens WhatsApp worden er sinds oktober 2011 via de app meer dan een miljard berichten per dag verstuurd.<sup>7</sup>

Whatsapp is ook in Nederland een van de meest populaire apps<sup>8</sup> met miljoenen Nederlandse gebruikers.<sup>9</sup> De app is zo bekend dat het werkwoord 'whatsappen' sinds

---

<sup>1</sup> URL: <http://www.whatsapp.com/>.

<sup>2</sup> 3561 Homestead Road, #416, Santa Clara, Californië 95010-5161.

<sup>3</sup> URL: <http://www.whatsapp.com/legal/> (versie 7 juli 2012).

<sup>4</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 2.

<sup>5</sup> URL: <https://itunes.apple.com/nl/app/whatsapp-messenger/id310633997>.

<sup>6</sup> Zie o.a. URL: <https://play.google.com/store/apps/details?id=com.whatsapp&hl=nl>; <http://www.windowsphone.com/nl-nl/store/app/whatsapp/218a0ebb-1585-4c7e-a9ec-054cf4569a79>.

<sup>7</sup> URL: <http://blog.whatsapp.com/index.php/2011/10/one-billion-messages/>.

<sup>8</sup> URL: <http://www.intelligence-group.nl/nl/actueel/augustus-2012/nieuws/facebook-en-whatsapp-meest-populaire-apps-onder-nederlandse-beroepsbevolking>.

<sup>9</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 3.

[VERTROUWELIJK: (...)]

**Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: (...)]

oktober 2012 aan de Van Dale (Van Dale Groot woordenboek van de Nederlandse taal) is toegevoegd.<sup>10</sup>

#### *Onderzoeksvragen*

Het onderzoek heeft zich geconcentreerd op de volgende vragen:

- Zijn de gegevens die WhatsApp in het kader van de app verzamelt persoonsgegevens, zoals gedefinieerd in artikel 1, aanhef en onder a, van de Wet bescherming persoonsgegevens (Wbp)?
- Heeft WhatsApp een grondslag voor de verwerking van de mobiele telefoonnummers van niet-gebruikers die zijn opgenomen in het adresboek van whatsapp-gebruikers als bedoeld in artikel 8 van de Wbp?
- Heeft WhatsApp een grondslag voor de verwerking van statusberichten als bedoeld in artikel 8 van de Wbp?
- Is het nodig dat WhatsApp alle mobiele telefoonnummers in het adresboek van whatsapp-gebruikers verzamelt en vervolgens verwerkt (artikel 11, eerste lid, van de Wbp: bovenmatigheid)?
- Worden de gegevens van whatsapp-gebruikers langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (artikel 10 van de Wbp)?
- Heeft WhatsApp passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen, bijvoorbeeld tegen onbevoegde kennisneming van berichten die via de app worden verstuurd als bedoeld in artikel 13 van de Wbp?

#### *Verloop onderzoek*

Voorafgaand aan het onderzoek hebben het CBP en de OPC een *Memorandum of Understanding* (samenwerkingsovereenkomst; hierna: MoU) gesloten met betrekking tot de wederzijdse uitwisseling van onderzoeksgegevens. De overeenkomst is in werking getreden op 16 januari 2012. Het CBP en de OPC hebben tijdens dit onderzoek onder deze MoU onderzoeksgegevens gedeeld.<sup>11</sup>

Het CBP heeft WhatsApp bij brief van 16 februari 2012 schriftelijk ingelicht een onderzoek in te stellen naar de verwerking van persoonsgegevens in het kader van de app en om inlichtingen verzocht. WhatsApp heeft bij brief van 22 maart 2012 geantwoord.

Het CBP heeft bij brief van 9 mei 2012 om nadere inlichtingen verzocht. WhatsApp heeft de gevraagde inlichtingen op 17 mei 2012 bij brief aan het CBP verstrekt.

---

<sup>10</sup> 'Whatsappen opgenomen in Van Dale', *Nu.nl* 19 september 2012. URL: <http://www.nu.nl/internet/2913592/whatsappen-opgenomen-in-van-dale.html>. Zie ook 'Whatsappen' als werkwoord in Dikke Van Dale', *whatsappen.nl* 19 september 2012, geüpdatet op 17 oktober 2012. URL: <http://www.whatsappen.nl/nieuws/2012/09/19/whatsappen-in-grote-of-dikke-van-dale/>.

<sup>11</sup> Op grond van artikel 2:5 van de Awb mag eenieder die betrokken is bij de uitvoering van de taak van het CBP vertrouwelijke gegevens openbaar maken voor zover dit noodzakelijk is voor een goede uitvoering van de bestuurstaak.

Het CBP heeft in maart en augustus 2012 digitaal onderzoek verricht naar de app.<sup>12</sup> De privacy policy<sup>13</sup> en de voorwaarden<sup>14</sup> zijn forensisch vastgelegd. De app is geïnstalleerd op smartphones<sup>15</sup> op naam van het CBP en er zijn foto's/screenshots gemaakt van het installatieproces en de gebruiksmogelijkheden van de app. Er zijn berichten uitgewisseld tussen de smartphones en de beveiliging van het berichtenverkeer is geanalyseerd met packet analyse software.<sup>16</sup>

Het CBP heeft zijn rapport Voorlopige Bevindingen van 2 oktober 2012 op 15 oktober 2012 aan WhatsApp verzonden, gelijktijdig met de voorlopige bevindingen van de OPC. Bij het rapport Voorlopige Bevindingen is een informele Engelse vertaling gevoegd. Het CBP heeft WhatsApp in de gelegenheid gesteld om haar zienswijze op het rapport naar voren te brengen.

WhatsApp heeft bij e-mail van 30 oktober 2012 om uitstel gevraagd van de termijn voor het geven van een zienswijze. Bij e-mail van 31 oktober 2012 heeft de OPC, mede namens het CBP, WhatsApp bericht dat uitstel werd verleend tot en met 30 november 2012. Bij e-mail van 29 november 2012 heeft WhatsApp haar zienswijze gegeven op het rapport Voorlopige Bevindingen.

Op 4 en 5 december 2012 heeft de OPC, in samenspraak met het CBP, (per e-mail en telefonisch) contact opgenomen met de advocaat-gemachtigde van WhatsApp met het verzoek om een reactie op een in de media geconstateerd probleem met de beveiliging. WhatsApp heeft een toelichting gegeven bij e-mail van 7 december 2012. Bij e-mail van 10 december 2012 heeft de OPC, in samenspraak met het CBP, aanvullende vragen gesteld aan WhatsApp naar aanleiding van haar zienswijze, met een verzoek om in dat verband op korte termijn mee te werken aan een video *conference call*. Bij e-mail van 17 december 2012 heeft WhatsApp positief gereageerd op het verzoek. Bij e-mails van 18 december 2012 heeft de OPC, in samenspraak met het CBP, de aanvullende vragen nader toegelicht. Bij e-mail van 19 december 2012 heeft WhatsApp twee diagrammen toegestuurd met nadere informatie. Bij e-mail van 20 december 2012 heeft de OPC, in samenspraak met het CBP, gevraagd om een toelichting op de diagrammen. WhatsApp heeft bij e-mail van 20 december 2012 een toelichting verstrekt.

Het CBP heeft in december 2012 en januari 2013 opnieuw digitaal onderzoek gedaan naar de app. Daarbij is de wachtwoordbeveiliging geanalyseerd en zijn foto's/screenshots gemaakt van het installatieproces en de gebruiksmogelijkheden van

---

<sup>12</sup> Op grond van artikel 5:18 van de Awb zijn toezichthouders onder meer bevoegd zaken (zoals bijvoorbeeld smartphones) te onderzoeken en aan opname te onderwerpen (inclusief het maken van foto's/screenshots). Zie *Tekst & Commentaar AWB*: aantekening 3B bij artikel 5:18 van de Awb.

<sup>13</sup> URL: <http://www.whatsapp.com/legal/#Privacy>.

<sup>14</sup> URL: <http://www.whatsapp.com/legal/#TOS>.

<sup>15</sup> De app is geïnstalleerd op drie smartphones met de besturingssystemen: Android, iOS en Windows. De app is niet getest op Nokia en BlackBerry.

<sup>16</sup> URL: <https://www.wireshark.org/>.



de (nieuwste versies van de) app.<sup>17</sup> Op 4 januari 2013 heeft een conference call plaatsgevonden tussen het CBP, de OPC en WhatsApp en haar advocaat-gemachtigde. De OPC heeft, in samenspraak met het CBP, bij e-mail van 5 januari 2013 een nadere toelichting gevraagd aan WhatsApp. Bij e-mail van 5 januari 2013 heeft WhatsApp een reactie gegeven op deze e-mail.

Het CBP heeft het rapport Definitieve Bevindingen op 15 januari 2013 vastgesteld.

#### *Zienswijze van WhatsApp*

In haar zienswijze (inclusief daaropvolgende e-mailcorrespondentie en de conference call van 4 januari 2013) brengt WhatsApp, samengevat weergegeven, naar voren dat 'out-of-network' telefoonnummers (dat wil zeggen: nummers van niet-gebruikers van de app) op de whatsapp servers worden geanonimiseerd en gehasht op een manier die het extreem moeilijk maakt voor WhatsApp (of derden) om de originele nummers te achterhalen. WhatsApp geeft aan dat volgens haar in zoverre (al) sprake is van een *compare and forget* systeem.<sup>18</sup>

Ten aanzien van het automatisch genereren van het wachtwoord geeft WhatsApp aan dat zij haar werkwijze heeft aangepast, in die zin dat er app updates beschikbaar zijn die niet langer het WiFi MAC-adres of het IMEI-toestelnummer gebruiken, maar [VERTROUWELIJK: (...)].<sup>19</sup>

Verder wijst WhatsApp erop dat gebruikers in de laatste iOS versie van de app (volgens WhatsApp het meest gebruikte besturingssysteem voor de app) de mogelijkheid hebben om WhatsApp geen toegang te geven tot hun elektronische adresboek. Indien gebruikers, via een dialoogbox opgeroepen door het besturingssysteem, WhatsApp toegang weigeren tot hun adresboek, kunnen zij handmatig een telefoonnummer invoeren om die persoon een whatsapp-bericht te versturen. Ten aanzien van toegang tot het adresboek op smartphones met andere besturingssystemen geeft WhatsApp aan geen meerwaarde te zien in het ontwikkelen van een toestemmingsvraag in de app zelf.<sup>20</sup> Volgens WhatsApp verleent de gebruiker toestemming voor toegang tot het adresboek door de app te installeren.<sup>21</sup>

WhatsApp geeft in haar zienswijze aan dat zij bezig is potentiële kandidaten te identificeren om aan te wijzen als haar vertegenwoordiger in Nederland.<sup>22</sup>

Van inactieve gebruikers (bijvoorbeeld gebruikers die (eenmalig) gratis whatsapp installeren en uitproberen en er vervolgens geen gebruik meer van maken) bewaart WhatsApp nog gedurende een jaar gegevens. Volgens WhatsApp moet zij, met name

---

<sup>17</sup> Het betreft de whatsapp-versies 2.8.9108 voor Android, gelanceerd op 8 december 2012, 2.8.7 voor iOS, gelanceerd op 7 december 2012 en 2.8.10.0 voor Windows, gelanceerd op 19 december 2012.

<sup>18</sup> Zienswijze WhatsApp van 29 november 2012, p. 1.

<sup>19</sup> Idem, p. 2.

<sup>20</sup> E-mail WhatsApp aan de OPC van 4 januari 2013.

<sup>21</sup> Idem.

<sup>22</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

als het om een betaald account gaat, de gegevens bewaren gedurende de *subscription* periode voor een goede dienstverlening zonder kwaliteitsverlies (tenzij het gaat om gegevens verwijderd door de gebruiker voor de vervaldatum).<sup>23</sup>

WhatsApp geeft in haar zienswijze aan dat het toevoegen van een waarschuwing/pop-up over de verspreiding van statusberichten - als gebruikers hun statusbericht aanpassen - op de agenda voor productontwikkeling staat.<sup>24</sup>

Ten slotte schrijft WhatsApp in algemene zin te gaan werken aan bewaartermijnen en de informatie daarover.<sup>25</sup>

In dit rapport is de zakelijke inhoud van de zienswijze van WhatsApp opgenomen per onderdeel, met de reactie daarop van het CBP en of de reactie heeft geleid tot aanpassing van de bevindingen en daarmee samenhangende wijziging(en) in de conclusies.

## 2. BEVINDINGEN

### 2.1 Whatsapp installeren en gebruiken

Eenieder kan de whatsapp-app downloaden uit diverse online app-winkels. Aanschaf van whatsapp voor de iPhone kost eenmalig 0,89 (bij aanvang van het onderzoek: 0,79) eurocent. Op andere besturingssystemen is de app gratis gedurende een proefperiode van één jaar. Het verzenden en ontvangen van berichten via de app is gratis. Gebruikers betalen alleen de kosten voor het datagebruik via internet.

De app is toegankelijk voor en (mede) gericht op personen in Nederland. Dit blijkt onder meer uit het feit dat WhatsApp de veel gestelde vragen (FAQ) beschikbaar stelt in het Nederlands, evenals diverse dialoogboxen en instellingsschermen.<sup>26</sup> Ook de standaardtekst voor het uitnodigen van nieuwe contacten is opgesteld in het Nederlands.

---

<sup>23</sup> Idem.

<sup>24</sup> Idem.

<sup>25</sup> Idem, p. 3.

<sup>26</sup> URL: <http://www.whatsapp.com/faq/>. Bij aanvang van het onderzoek: URL: <http://www.whatsapp.com/faq/?l=nl>. Het CBP heeft tijdens het onderzoek vastgesteld dat ook de telefonische verificatieprocedure in het Nederlands geschiedt, als SMS-authenticatie mislukt.



**Figuur 1** Standaardtekst voor het uitnodigen van nieuwe contacten

WhatsApp doet daarnaast een specifieke oproep aan Nederlandse vertalers. Deze luidt thans:

*"Help translate WhatsApp today! We're looking for translators in: Arabic, Danish, Dutch, Farsi, Filipino, Finnish, French, German, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese (Brazil), Russian, Simplified Chinese, Spanish, Swedish, Thai, Traditional Chinese, Turkish, Urdu, and many more languages."*<sup>27</sup>

Nadat de app is gedownload, dient een gebruiker de app te installeren. Hem wordt gevraagd om de app toegang te geven tot verschillende smartphone systeemhulpprogramma's, zoals lees- en schrijftoegang (hierna: toegang) tot het adresboek, internettoegang voor het maken van netwerksockets, nauwkeurige (GPS) locatie, schrijven naar microSD opslag, maar ook tot functies als 'Audio opnemen', 'SMS berichten verzenden', 'Telefoonnummers rechtstreeks bellen' en 'Automatisch starten bij opstarten'.<sup>28</sup>

Na installatie dient de gebruiker zich met zijn smartphone te registreren bij WhatsApp.

Gedurende het registratieproces wordt de gebruiker eerst verzocht om de algemene voorwaarden en het privacybeleid van het bedrijf te lezen en te accepteren (hierna gezamenlijk te noemen: de voorwaarden).

Zodra een gebruiker de voorwaarden heeft gelezen en geaccepteerd wordt hem gevraagd aan te geven in welk land hij woont en wordt hem ook gevraagd zijn mobiele telefoonnummer op te geven. In sommige gevallen vraagt de app de naam die een gebruiker heeft ingesteld voor *push* berichten (van toepassing bij iPhones en Windows Phones).

<sup>27</sup> URL: <http://translate.whatsapp.com/>.

<sup>28</sup> De vraag of de toegang tot andere systeemhulpprogramma's dan lees- en schrijftoegang tot het adresboek rechtmatig is, is niet door het CBP onderzocht. De toegang tot die andere systeemhulpprogramma's door de app op de smartphone valt buiten de scope van dit onderzoek.

Nadat de gebruiker zijn landcode en mobiele telefoonnummer heeft ingevoerd, verzamelt WhatsApp de volgende gegevens van de smartphone: het unieke klantnummer (IMSI), het mobiele telefoonnummer (MSISDN), de mobiele landcode (MCC) en de mobiele netwerk code (MNC). Het unieke IMSI-klantnummer, de mobiele landcode en de mobiele netwerk code worden na aanmaak van het account gedurende dertig dagen bewaard.<sup>29</sup>

WhatsApp maakt automatisch een gebruikers-ID en wachtwoord aan voor gebruikers. De gebruikers-ID is [VERTROUWELIJK: (...)], het wachtwoord was bij aanvang van het onderzoek gebaseerd op het unieke vijftiencijferige toestelnummer (IMEI). Alleen op de iPhone gebruikte het bedrijf een ander gegeven om het wachtwoord te genereren, namelijk het WiFi MAC-adres van de iPhone.<sup>30</sup> Naar aanleiding van het rapport Voorlopige Bevindingen heeft WhatsApp haar werkwijze met betrekking tot het aanmaken van wachtwoorden gewijzigd: app updates gebruiken in beginsel niet langer het WiFi MAC-adres of het IMEI-toestelnummer, maar [VERTROUWELIJK: (...)] (zie paragraaf 2.4.1).

Hierna stuurt WhatsApp een regulier sms-bericht met een activatiecode naar het opgegeven mobiele telefoonnummer. In bepaalde gevallen kan de gebruiker ervoor kiezen om te worden gebeld door een spraakcomputer, die de activatiecode vervolgens voorleest. De gebruiker dient de drie- of zescijferige activatiecode in te voeren om het telefoonnummer te verifiëren. Het bedrijf gebruikt de bevestiging van de gebruiker om te controleren of de gegevens die de gebruiker heeft verstrekt, overeenstemmen met de gegevens die WhatsApp van het mobiele apparaat heeft verzameld.

Na deze controle kan de gebruiker optioneel een profielnaam kiezen. Deze naam is niet de whatsapp-gebruikers-ID. De zelfgekozen naam wordt gebruikt als afzender in berichten die de gebruiker verstuurt. Tot slot wordt de gebruiker geregistreerd en kan hij beginnen met whatsappen.

## 2.2 Toegang tot het adresboek op de smartphone

WhatsApp vraagt bij installatie om toegang tot het adresboek van de gebruiker.<sup>31</sup> Zodra de gebruiker de app heeft geïnstalleerd, worden de mobiele telefoonnummers van alle contacten in het adresboek op de smartphone naar de whatsapp servers gestuurd.

---

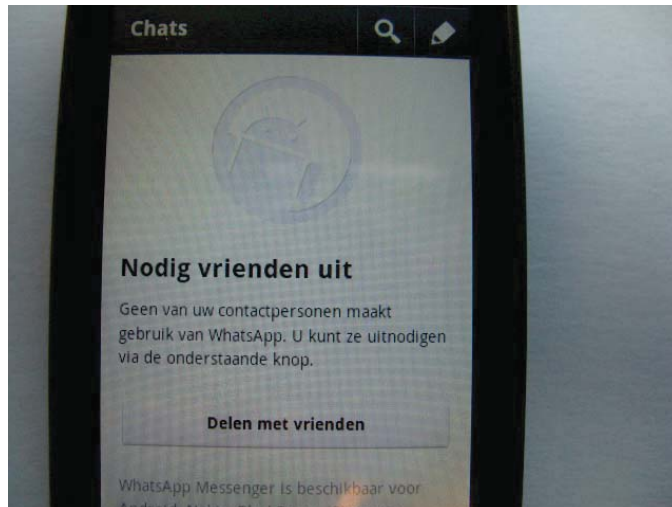
<sup>29</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 1.

<sup>30</sup> Een MAC-adres is een uniek nummer dat door de fabrikant is vastgelegd in de hardware van apparatuur, in dit geval in de ingebouwde WiFi netwerkkartaal in de smartphone. MAC staat voor *Medium Access Control*.

<sup>31</sup> Technisch gezien vraagt het besturingssysteem om een machtiging voordat de app wordt geïnstalleerd, dat wil zeggen op smartphones met het Windows en Android besturingssysteem. Er verschijnt op deze smartphones in de app zelf geen aparte toestemmingsvraag voor toegang tot het adresboek.

Bij aanvang van het onderzoek was het niet mogelijk de app te installeren zonder toegang te bieden tot het volledige adresboek.<sup>32</sup> Het was evenmin mogelijk om individuele contacten te selecteren, een functionaliteit die bij andere veelgebruikte communicatie-programma's (inclusief chatberichtendiensten) wel beschikbaar was en is.

Indien het adresboek leeg is, wordt de gebruiker gevraagd om anderen uit te nodigen via standaard-sms of e-mail (zie Figuur 2).



**Figuur 2** Scherm op Android indien geen van de contacten in het adresboek een whatsapp-gebruiker is



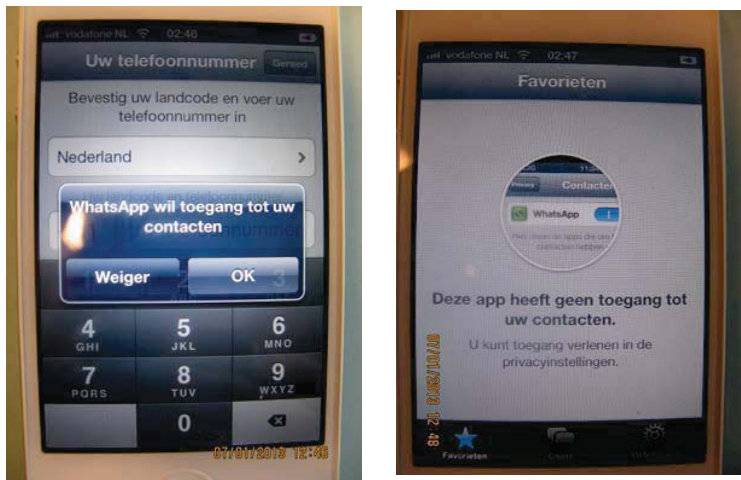
**Figuur 3** Dialogscherm voor verplichte toegang tot adresboek op de iPhone

<sup>32</sup> Het CBP heeft dit vastgesteld in september 2012 voor Android versie 2.8.4771, voor iPhone versie 2.8.4 en voor Windows Phone versie 2.8.2.0.

Bij het doorlopen van het installatieproces op de iPhone leek het in eerste instantie wel mogelijk om de app te installeren zonder toegang tot het adresboek te verlenen. In het eerste dialoogscherf kon de gebruiker kiezen voor de optie 'Sta niet toe'. In een later dialoogscherf voor het opslaan van 'Favorieten' (voorkeurscontacten waarmee de gebruiker wil whatsappen) vroeg WhatsApp echter alsnog toegang tot het adresboek. Omdat dit scherm alleen de knop 'Sta toe' bevatte, zonder mogelijkheid het scherm te sluiten, kon de gebruiker in de praktijk de toegang tot zijn adresboek niet weigeren.

In reactie op het rapport Voorlopige Bevindingen heeft WhatsApp naar voren gebracht dat in de laatste iOS versie van de app (volgens WhatsApp het meest gebruikte besturingssysteem voor de app) de gebruiker wel de mogelijkheid heeft (i) WhatsApp geen toegang te geven tot zijn adresboek en (ii) zelf een telefoonnummer in te voeren om een whatsapp-bericht te versturen. WhatsApp heeft naderhand verklaard geen meerwaarde te zien in het ontwikkelen van een toestemmingsvraag in de app zelf op smartphones met andere besturingssystemen dan iOS.<sup>33</sup> Volgens WhatsApp verleent de gebruiker toestemming voor toegang tot het adresboek door de app te installeren.<sup>34</sup>

Het CBP heeft begin januari 2013 vastgesteld dat de gebruiker op een iPhone met besturingssysteem iOS versie 6 inderdaad de app kan installeren en gebruiken zonder toegang tot het adresboek. Het dialoogscherf waarmee tijdens het doorlopen van het installatieproces toegang wordt gevraagd tot het adresboek bevat zowel de knop 'Weiger' als 'OK'.<sup>35</sup>



**Figuur 4** Dialoogschermen voor optionele toegang tot adresboek op de iPhone

<sup>33</sup> E-mail WhatsApp aan de OPC van 4 januari 2013.

<sup>34</sup> Idem.

<sup>35</sup> Het CBP heeft dit gecontroleerd en vastgesteld voor whatsapp-versie 2.8.7, op een iPhone met besturingssysteem iOS 6.0.1.

Als de gebruiker de toegang tot zijn adresboek weigert, kan hij de app (desondanks) gebruiken door zelf een telefoonnummer in te voeren om een bericht te versturen naar een andere whatsapp-gebruiker en/of nieuwe contacten uit te nodigen.

WhatsApp heeft verklaard dat het adresboek [VERTROUWELIJK: (...)] wordt verzonden naar de servers, of op het moment dat de gebruiker een wijziging in zijn adresboek handmatig doorgeeft aan WhatsApp (verversing).<sup>36</sup> WhatsApp doet dit om de gebruiker te tonen welke van zijn contacten alsnog whatsapp zijn gaan gebruiken.<sup>37</sup>

WhatsApp heeft verklaard dat het bedrijf uit het adresboek alleen de mobiele telefoonnummers verzamelt, geen andere gegevens zoals namen, e-mailadressen, adresgegevens of andere informatie.<sup>38</sup>

Op de servers worden de mobiele telefoonnummers aangemerkt als 'in-network' of 'out-of-network'. 'In-network' telefoonnummers zijn nummers van betrokkenen die gebruik maken van whatsapp. Gebruikers kunnen alleen berichten sturen aan andere 'in-network' nummers. 'Out-of-network' telefoonnummers zijn nummers van niet-gebruikers van de app.

Volgens WhatsApp worden 'in-network' nummers op de servers bewaard [VERTROUWELIJK: (...)]. 'Out-of-network' nummers worden opgeslagen met een cryptografische [VERTROUWELIJK: (...)] hash (unieke hashwaarde met een vaste lengte).<sup>39</sup> [VERTROUWELIJK: (...)] WhatsApp verklaarde deze gegevens van niet-gebruikers ('out-of-network') permanent te bewaren, tot zij alsnog whatsapp-gebruikers werden.<sup>40</sup>

In reactie op het rapport Voorlopige Bevindingen heeft WhatsApp verklaard dat 'out-of-network' telefoonnummers op de whatsapp servers worden geanonimiseerd en gehasht op een manier die het extreem moeilijk maakt voor WhatsApp (of derden) om de originele nummers te achterhalen. Bij e-mail van 20 december 2012, zoals nader toegelicht tijdens de conference call van 4 januari 2013, heeft WhatsApp aangegeven hoe de hash van 'out-of-network' nummers door haar wordt berekend.  
[VERTROUWELIJK: (...)].<sup>41</sup>[VERTROUWELIJK: (...)]

Als een niet-gebruiker alsnog whatsapp gaat gebruiken, voegt WhatsApp automatisch zijn telefoonnummer toe aan de lijst whatsapp-gebruikers ('in-network') op de smartphones van alle gebruikers die dit nummer in hun adresboek hebben staan, en aan het 'in-network' bestand op de eigen servers.

---

<sup>36</sup> Reactie WhatsApp op verzoek om inlichtingen van 22 maart 2012, p. 2. Zie ook Zienswijze WhatsApp van 29 november 2012, p. 1.

<sup>37</sup> Reactie WhatsApp op verzoek om inlichtingen van 22 maart 2012, p. 1.

<sup>38</sup> Idem.

<sup>39</sup> [VERTROUWELIJK: (...)] Hashen is een wiskundige bewerking die van informatie (bijvoorbeeld tekst) een unieke hashcode maakt die altijd even lang is (bijvoorbeeld 128 bits). Het maakt daarbij niet uit hoe groot de oorspronkelijke tekst is.

<sup>40</sup> Idem.

<sup>41</sup> E-mail WhatsApp van 20 december 2012.

Elke gebruiker kan selectief contacten met andere whatsapp-gebruikers blokkeren.

### 2.3 Bewaartermijnen gegevens van whatsapp-gebruikers

WhatsApp heeft verklaard dat het bedrijf succesvol afgeleverde berichten niet bewaart. Deze berichten zijn alleen beschikbaar op de smartphones van de verzenders en de ontvangers daarvan.<sup>42</sup>

#### **Berichten bewaard op de whatsapp servers**

Niet-succesvol afgeleverde berichten worden gedurende dertig dagen op de servers bewaard.<sup>43</sup> Na aflevering wordt het bericht alsnog automatisch van de servers verwijderd. Op de servers worden de niet-succesvol afgeleverde berichten opgeslagen [VERTROUWELIJK: (...)].

#### **Berichten bewaard op de smartphone**

De gebruiker kan zelf gegevens wissen op zijn eigen smartphone, zoals de berichten die hij met een andere gebruiker heeft gewisseld. Een gebruiker kan er ook voor kiezen alle verzonden en ontvangen berichten op zijn smartphone te wissen. Daarmee zijn de gegevens nog niet definitief verdwenen. WhatsApp maakt op Android smartphones automatisch [VERTROUWELIJK: (...)] een reservekopie.<sup>44</sup> Het is op de Nokia en Android smartphones mogelijk om de recent gewiste chats terug te zetten, door de app te deïnstalleren en opnieuw te installeren. Tijdens de (her-) installatie wordt de back-up herkend en automatisch de vraag aan de gebruiker voorgelegd of de back-up teruggezet dient te worden. Een gebruiker kan er bij een iPhone voor kiezen om zelf een back-up te maken van bepaalde gegevens, door te synchroniseren met iTunes of iCloud.

#### **Account gegevens bewaard op de whatsapp servers<sup>45</sup>**

De gebruiker kan zijn whatsapp-account opheffen door gebruik te maken van de optie 'Account verwijderen' in het instellingsmenu van de app. WhatsApp heeft bevestigd dat een aantal gegevens van deze gebruiker dan onmiddellijk wordt verwijderd uit het whatsapp-systeem.<sup>46</sup> Het betreft de volgende gegevens:

- het verwijderen van het mobiele telefoonnummer van de gebruiker uit de whatsapp Favorietenlijst van andere whatsapp-gebruikers;
- het verwijderen van de whatsapp-gebruiker uit alle whatsapp-groepen;
- het verwijderen van de berichtengeschiedenis op het mobiele apparaat.

WhatsApp heeft verklaard betalingsgegevens nog dertig dagen te bewaren nadat een gebruiker zijn account heeft opgeheven.<sup>47</sup> Het betreft het accounttype (gratis of

---

<sup>42</sup> Reactie WhatsApp op verzoek om inlichtingen van 22 maart 2012, p. 2.

<sup>43</sup> Idem, p. 2.

<sup>44</sup> [VERTROUWELIJK: (...)]

<sup>45</sup> Naleving van het bepaalde in artikel 10 van de Wbp (bewaartermijn) valt alleen binnen de scope van dit onderzoek voor zover het account gegevens van inactieve gebruikers betreft.

<sup>46</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 2.

<sup>47</sup> Idem.



betaald), zijn telefoonnummer en de beëindigings-/vervaldatum van de afgenomen dienst.<sup>48</sup> Als reden voor deze bewaartermijn noemt WhatsApp het vergemakkelijken van een hernieuwde registratie door de gebruiker, als de gebruiker bijvoorbeeld spijt heeft gekregen van zijn besluit om zijn account op te heffen.

Als een gebruiker zijn account niet meer gebruikt, maar er niet voor kiest om zijn account op te heffen, bewaart WhatsApp de gegevens van de gebruiker gedurende een jaar.<sup>49</sup> Dit geldt bijvoorbeeld voor de gebruikers die de app (op andere smartphones dan de iPhone) een jaar lang gratis hebben gebruikt. Als ze na het verstrijken van dat eerste jaar niet betalen voor de app, worden hun gegevens nog een jaar lang bewaard. Deze bewaartermijn is bijvoorbeeld ook van toepassing op gebruikers die van smartphone of mobiele telefoonnummer wisselen, maar hun account niet opheffen.

WhatsApp stelt zich in haar zienswijze op het standpunt dat zij, met name als het om een betaald account gaat, de gegevens moet bewaren gedurende de *subscription* periode voor een goede dienstverlening zonder kwaliteitsverlies (tenzij het gaat om gegevens verwijderd door de gebruiker voor de vervaldatum).<sup>50</sup>

## 2.4 Beveiliging

### 2.4.1 Automatisch genereren van het wachtwoord

WhatsApp maakt automatisch een gebruikers-ID en wachtwoord aan voor gebruikers. De gebruikers-ID is [VERTROUWELIJK: (...)], het wachtwoord was bij aanvang van het onderzoek gebaseerd op het unieke IMEI-toestelnummer (zie ook paragraaf 2.1). Om het wachtwoord op de smartphone te genereren werd het IMEI [VERTROUWELIJK: (...)] omgezet naar een unieke hashwaarde met een vaste lengte. [VERTROUWELIJK: (...)]

Op de iPhone gebruikte WhatsApp een andere methode. Daar werd het WiFi MAC-adres gebruikt om [VERTROUWELIJK: (...)] een wachtwoord te genereren. De [VERTROUWELIJK: (...)] hashwaarde werd berekend door het MAC-adres [VERTROUWELIJK: (...)] te hashen.<sup>51</sup>

Het CBP heeft tijdens het onderzoek kennis genomen van beveiligingswaarschuwingen over het aanmaken van wachtwoorden.<sup>52</sup> Met behulp van het mobiele telefoonnummer en een (gereproduceerd) wachtwoord kon iedereen, bij aanvang van het onderzoek, de berichten inzien van een whatsapp-gebruiker en uit

---

<sup>48</sup> Het CBP heeft geen aanwijzingen dat WhatsApp andere soorten betalingsgegevens verzamelt en verwerkt, zoals creditcard nummers etc.

<sup>49</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 2.

<sup>50</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

<sup>51</sup> [VERTROUWELIJK: (...)]

<sup>52</sup> 'WhatsApp accounts almost completely unprotected', *h-online.com* 14 september 2012. ' URL: <http://www.h-online.com/security/news/item/WhatsApp-accounts-almost-completely-unprotected-1708545.html>.

diens naam berichten versturen (zie hierover verder paragraaf 3.9).  
[VERTROUWELIJK: (...)]

Naar aanleiding van het rapport Voorlopige Bevindingen heeft WhatsApp verklaard haar werkwijze met betrekking tot het aanmaken van wachtwoorden te hebben gewijzigd, in die zin dat zij in december 2012 updates van de app heeft uitgebracht die in beginsel niet langer het WiFi MAC-adres of het IMEI-toestelnummer gebruiken maar [VERTROUWELIJK: (...)].<sup>53</sup> [VERTROUWELIJK: (...)]

Bij actieve gebruikers forceert WhatsApp dat zij gebruik maken van de nieuwste versies, door het verlopen van de oude(re) versies van whatsapp.<sup>54</sup> WhatsApp heeft verklaard dat zij verwacht dat medio februari 2013 alle actieve gebruikers overgestapt zijn naar de nieuwste versies van de app.<sup>55</sup> Een inactieve whatsapp-gebruiker (bijvoorbeeld een gebruiker die (eenmalig) gratis whatsapp installeert en uitprobeert en er vervolgens geen gebruik meer van maakt) wordt echter niet geconfronteerd met deze 'gedwongen update'.

Het CBP heeft in december 2012 de wachtwoordbeveiliging geanalyseerd en met behulp van digitaal onderzoek met de smartphones op naam van het CBP vastgesteld dat WhatsApp de wachtwoordbeveiliging inderdaad heeft gewijzigd.<sup>56</sup> Het CBP heeft eveneens vastgesteld dat in geval van de verlopen versies van inactieve gebruikers (toch) nog whatsapp-berichten konden worden onderschept en gelezen met behulp van [VERTROUWELIJK: (...)] een (gereproduceerd) wachtwoord (op basis van het WiFi MAC-adres of het IMEI-toestelnummer).<sup>57</sup>

WhatsApp heeft in de conference call van 4 januari 2013 erkend dat er een risico blijft voor inactieve gebruikers, en aangegeven dat het remediëren daarvan op de agenda voor productontwikkeling komt te staan, zonder daarbij een termijn te noemen.

#### 2.4.2 Beveiliging van de gegevensoverdracht via internet

Het CBP heeft begin 2012 kennis genomen van beveiligingswaarschuwingen over problemen met de gegevensoverdracht via internet. Door het ontbreken van versleuteling van de gegevensoverdracht via internet zou het mogelijk zijn voor onbevoegden om kennis te nemen van mobiele telefoonnummers en de inhoud van berichten.<sup>58</sup>

---

<sup>53</sup> Zienswijze WhatsApp van 29 november 2012, p.2.

<sup>54</sup> Het CBP heeft dit vastgesteld voor Android 2.8.9108 en Windows Phone versie 2.8.10. Ook iPhone versie 2.8.4 is inmiddels verlopen.

<sup>55</sup> Verklaring WhatsApp tijdens conference call van 4 januari 2013.

<sup>56</sup> Het CBP heeft dit gecontroleerd voor Android versie 2.8.4771, voor iPhone versie 2.8.4 en voor Windows Phone versie 2.8.2.0.

<sup>57</sup> Idem.

<sup>58</sup> Zie bijvoorbeeld de waarschuwing van Secunia, een internationaal IT security bedrijf gespecialiseerd in *vulnerability management* (het opsporen van tekortkomingen in de beveiliging van software) en gevestigd in Kopenhagen, Denemarken.  
URL: <https://secunia.com/advisories/product/39212/>.

Bij aanvang van het onderzoek heeft de OPC met netwerkanalysesoftware vastgesteld dat er geen versleuteling werd toegepast op berichten die verstuurd werden met de app.<sup>59</sup> Daardoor was het mogelijk voor anderen om berichten te onderscheppen en te lezen als de gebruiker op een openbaar WiFi netwerk zat.

Naar aanleiding van de onderzoeksvragen van het CBP en de OPC over de getroffen beveiligingsmaatregelen heeft WhatsApp verklaard (nieuwe) end-to-end encryptie te hebben ingevoerd. Sinds mei 2012 versleutelt WhatsApp de inhoud van berichten.<sup>60</sup> Daartoe heeft het bedrijf nieuwe software ontwikkeld voor alle typen smartphones waarvoor de app beschikbaar is. Het CBP heeft vastgesteld dat de berichten via de app sinds medio mei 2012 op versleutelde wijze worden verzonden.<sup>61</sup>

## 2.5 Statusberichten

Een statusbericht is een boodschap van maximaal 139 karakters waarmee een gebruiker zijn status kan weergeven. Een voorbeeld van een statusbericht is 'beschikbaar' of 'druk bezig'. De app geeft elke gebruiker automatisch een statusbericht, dat zichtbaar is voor alle andere whatsapp-gebruikers die het mobiele telefoonnummer van de gebruiker in hun adresboek hebben staan. Een gebruiker kan het automatisch verzenden van het statusbericht naar individuele whatsapp-gebruikers onderdrukken door deze andere whatsapp-gebruikers op te nemen in een blokkeringslijst, maar die blokkering betreft alleen mensen waarvan hij het mobiele telefoonnummer kent. Zijn telefoonnummer kan daarnaast in vele andere adresboeken staan, van hem onbekende whatsapp-gebruikers.<sup>62</sup>

De standaardinstelling voor statusberichten is: *"Hey there! I am using WhatsApp"* (zie Figuur 5). Een gebruiker kan dit bericht wijzigen via het menu van de app. In het statusmenu zijn een aantal standaardmogelijkheden beschikbaar, maar een gebruiker kan ook zelf tekst invoeren om een eigen statusbericht maken. Dergelijke zelfgemaakte statusberichten kunnen ook gevoelige gegevens betreffen, zoals de exacte locatie waar de gebruiker verblijft, of mededelingen over zijn gezondheid.

Door handmatig weer de standaardtekst in te voeren kan een gebruiker het standaardbericht weer aanzetten. Eenmaal ingevoerde teksten blijven via het menu beschikbaar. De gebruiker kan daardoor via het menu desgewenst ook het standaardbericht weer aanzetten. Alleen op de iPhone kan de status met een aparte knop gewist worden (en dus leeg blijven).

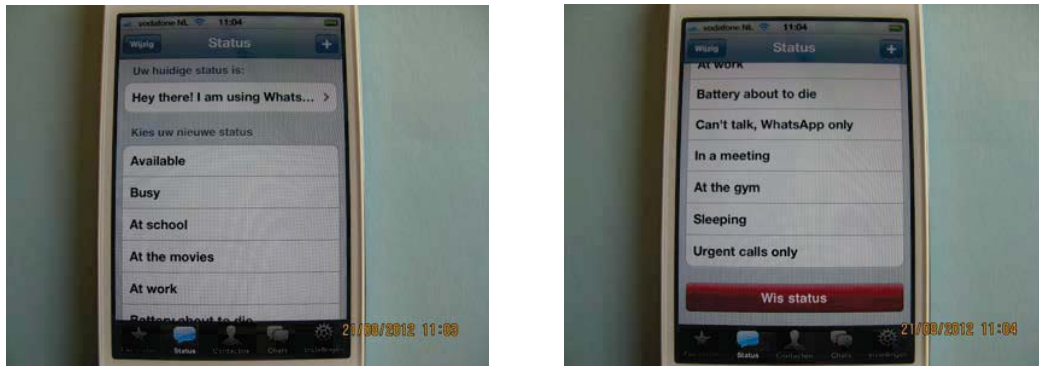
---

<sup>59</sup> De OPC heeft op 13 januari 2012 met behulp van packet analyse software vastgesteld dat de berichten in leesbare vorm werden verzonden en ontvangen.

<sup>60</sup> Reactie WhatsApp op verzoek om inlichtingen van 17 mei 2012, p. 2.

<sup>61</sup> Het CBP heeft de volgende softwareversies gecontroleerd: Android versie 2.8.1504, iOS versie 2.8.2, Windows Phone versie 2.8.00.

<sup>62</sup> Whatsapp voorwaarden van 7 juli 2012, paragraaf 5 onder A. URL: <http://www.whatsapp.com/legal/> (URL bezocht en forensisch vastgelegd op 26 september 2012 en 3 januari 2013).



**Figuur 5** Dialogscherm voor statusberichten

De voorwaarden van 5 januari 2012 bevatten een aparte paragraaf<sup>63</sup> over statusberichten ('*User Status Submissions*'). Naar aanleiding van het onderzoek van het CBP en de OPC heeft WhatsApp deze paragraaf uitgebreid. Gebruikers worden nu geïnformeerd over het feit dat hun status wordt gedeeld met alle andere gebruikers van de app die hun mobiele telefoonnummer in hun adresboek hebben staan. Deze informatie is toegevoegd aan de gebruiksvoorwaarden van 7 juli 2012.<sup>64</sup>

WhatsApp geeft in haar zienswijze aan dat het toevoegen van een waarschuwing/pop-up over de verspreiding van statusberichten - als gebruikers hun statusbericht aanpassen - op de agenda voor productontwikkeling staat.<sup>65</sup>

<sup>63</sup> Paragraaf 5 onder A bevatte op 5 januari 2012 de tekst: "*The WhatsApp Service permits the submission of status text and other communications submitted by you and other users ("User Status Submissions") and the hosting, sharing, and/or publishing of such User Status Submissions. As clarified in the following section, you retain your ownership rights in your User Status Submissions. You understand that whether or not such User Status Submissions are published, WhatsApp does not guarantee any confidentiality with respect to any submissions.*"

<sup>64</sup> De sinds 7 juli 2012 herziene tekst van Paragraaf 5 onder A luidt als volgt: "*The WhatsApp Service allows WhatsApp users to submit status text, profile photos and other communications submitted by you, as well as the automatic submission of your "last seen" status (collectively, the "Status Submissions"). These Status Submissions may be hosted, shared, and/or published as part of the WhatsApp Service, and may be visible to other users of the Service who have your mobile phone number in their mobile phone and which you have not expressly blocked. For clarity, direct messages, location data and photos or files that you send directly to other WhatsApp users will only be viewable by those WhatsApp user(s) or group(s) you directly send such information; but Status Submissions may be globally viewed by WhatsApp users that have your mobile phone number on their smartphone, unless the user is blocked by you. Currently, we have no method of providing different levels of visibility of your Status Submissions among users that have your mobile phone number – you acknowledge and agree that any Status Submissions may be globally viewed by users that have your mobile phone number, so don't submit or post status messages or profile photos that you don't want to be seen globally. A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service.*" URL: <http://www.whatsapp.com/legal/> (URL bezocht en forensisch vastgelegd op 26 september 2012 en 2 januari 2013).

<sup>65</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

### 3 UITWERKING VAN HET WETTELIJK KADER EN BEOORDELING

#### 3.1 Toepasselijk recht

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

Ingevolge artikel 4, eerste en tweede lid, van de Wbp is de wet van toepassing op de verwerking van persoonsgegevens (a) in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland of (b) door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de EU, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens. Dit artikel vormt een implementatie van artikel 4 van de Privacyrichtlijn 95/46/EG (hierna: Privacyrichtlijn).

Overweging 20 bij de Privacyrichtlijn luidt: *“Overwegende dat de vestiging in een derde land van de voor de verwerking verantwoordelijke de bescherming van personen waarin de onderhavige richtlijn voorziet, niet in de weg mag staan; dat in dit geval de verwerking moet worden geregeld door het recht van de Lid-Staat waarin de gebruikte middelen zich bevinden, en dat gewaarborgd moet worden dat de rechten en verplichtingen waarin de onderhavige richtlijn voorziet, in de praktijk worden geëerbiedigd”*.

Het begrip ‘gebruikte middelen’ in overweging 20 bij de Privacyrichtlijn impliceert (i) een activiteit die door de verantwoordelijke wordt uitgeoefend en (ii) het voornemen persoonsgegevens te verwerken.<sup>66</sup>

Onder het begrip ‘middelen’<sup>67</sup> wordt onder andere begrepen menselijke en/of technische middelen. Daaronder valt ook de verzameling van persoonsgegevens via de computers van gebruikers, bijvoorbeeld met cookies of JavaScript, of via mobiele apparaten van klanten door middel van specifieke software die op het apparaat is geïnstalleerd.<sup>68</sup> De voor de verwerking verantwoordelijke hoeft de middelen niet in eigendom of bezit te hebben om de verwerking binnen de werkingssfeer van de Wbp te laten vallen.<sup>69</sup>

De richtlijn betreffende privacy en elektronische communicatie 2002/58/EG (e-Privacyrichtlijn) regelt de bescherming van persoonsgegevens en van de persoonlijke

---

<sup>66</sup> WP29 Advies 8/2010 over toepasselijk recht, p. 20 en WP29 Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU van 30 mei 2002, p. 9. URL:

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf)  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf)

<sup>67</sup> Voor het begrip ‘equipment’ (‘apparatuur’) in de Engelse versie van de Privacyrichtlijn, wordt in andere EU-talen - zoals het Nederlands - het woord ‘middelen’ gebruikt. Dit is een argument voor een ruime uitleg van het begrip. WP29 Advies 8/2010 over toepasselijk recht, p. 8.

<sup>68</sup> Idem, p. 21. Zie ook WP29 Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU van 30 mei 2002, p. 11 e.v.

<sup>69</sup> Zie in dezelfde zin WP29 Advies 8/2010 over toepasselijk recht, p. 20.

levenssfeer voor gebruikers van openbare elektronische communicatiediensten. De bepalingen uit de e-Privacyrichtlijn (geïmplementeerd in de Telecommunicatiewet; hierna: Tw) geven aan bepaalde algemene normen uit de algemene Privacyrichtlijn (geïmplementeerd in de Wbp) een nadere invulling (bijvoorbeeld een nadere begrenzing/inperking van de toegestane verwerkingen). Er is geen sprake van een *lex specialis*-situatie: een bijzondere wet die gaat voor een algemene.<sup>70</sup>

#### Beoordeling

WhatsApp, met hoofdvestiging in Californië, en zonder kantoren buiten de Verenigde Staten, gebruikt smartphones van whatsapp-gebruikers - door middel van de app die op de apparaten is geïnstalleerd - als middel bij de verwerking van persoonsgegevens in het kader van de app (zie hierover paragraaf 3.5 van dit rapport).

De app is daarbij ook toegankelijk voor personen in Nederland. De dienst is ook (mede) gericht op personen in Nederland. Dit blijkt onder meer uit het feit dat WhatsApp diverse dialoogboxen en (instellings)schermen (waaronder de standaardtekst voor het uitnodigen van nieuwe contacten) evenals de veel gestelde vragen (FAQ) beschikbaar stelt in het Nederlands (zie paragraaf 2.1 van dit rapport). WhatsApp doet daarnaast een oproep aan Nederlandse vertalers om (verdere) informatie in het Nederlands te kunnen verstrekken.<sup>71</sup>

Gelet op het voorgaande is de Wbp van toepassing op de verwerking van persoonsgegevens in het kader van de app door WhatsApp (zoals nader begrensd/ingeperkt door de Tw, voor zover voor dit onderzoek van belang; zie hierover paragraaf 3.6 van dit rapport).

De Wbp is (evenals hoofdstuk 11 van de Tw) dwingend recht. Dit betekent dat de toepasselijkheid daarvan niet via een eenzijdige verklaring of contractueel in de algemene voorwaarden door WhatsApp kan worden uitgesloten.<sup>72</sup>

---

<sup>70</sup> Zie o.a. *Kamerstukken II 1999/2000*, 26 410, nr. 7, p. 2: “*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 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. (...)*”, (onderstreping toegevoegd door het CBP).

<sup>71</sup> URL: <http://translate.whatsapp.com/>.

<sup>72</sup> *Kamerstukken II 1997/1998*, 25 892, nr. 3, p. 10: “[Er, toevoeging door het CBP] (...) wordt aangenomen dat persoonlijkheidsrechten in beginsel niet overdraagbaar zijn en daarom niet voor contractuele afstand vatbaar zijn. Vanuit deze algemene notie gelden de voorschriften van de WBP als dwingend recht.” In de Terms of Service en Privacy Notice van Whatsapp, die alleen in het Engels beschikbaar zijn, wordt vermeld: “*You agree that: (i) the Whatsapp Service shall be deemed solely based in California; (ii) the Whatsapp Service shall be deemed a passive server that does not give rise to personal jurisdiction over Whatsapp, either specific or general, in jurisdictions other than California; and (iii) that you agree to subject to the jurisdiction of California in the event*

### 3.2 Bevoegdheid CBP

#### *Uitwerking van het wettelijk kader*

Ingevolge artikel 61, eerste lid, jo. artikel 51, eerste lid, van de Wbp heeft het CBP tot taak als toezichthouder toe te zien op (dat wil zeggen: heeft het jurisdictie ten aanzien van) de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde.

#### *Beoordeling*

Het CBP ziet aldus toe op de naleving van de bepalingen van de Wbp en (voor zover voor dit onderzoek van belang) van hoofdstuk 11 van de Tw voor zover het gaat om de verwerking van persoonsgegevens in de sector elektronische communicatie.<sup>73</sup> 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.

Gelet op het voorgaande (paragraaf 3.1 én paragraaf 3.2) heeft het CBP jurisdictie (dat wil zeggen: is het als toezichthouder bevoegd) ten aanzien van de verwerking van persoonsgegevens in het kader van de app door WhatsApp.

### 3.3 Verantwoordelijke

#### *Uitwerking van het wettelijk kader*

Op grond van artikel 1, aanhef en onder d, van de Wbp<sup>74</sup> is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

---

*of any legal dispute. These Terms of Service shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles. Any claim or dispute between you and Whatsapp that arises in whole or in part from the Whatsapp Service shall be decided exclusively by a court of competent jurisdiction located in Santa Clara County, California". En: "Special Note to International Users The WhatsApp Site and Service are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy Policy, and our Terms of Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes." URL:*

<http://www.whatsapp.com/legal/?l=nl>.

<sup>73</sup> *Kamerstukken II 2002/03, 28 851, nr. 7, p. 53-54.*

<sup>74</sup> Dit artikel vormt een implementatie van artikel 2, onder d, van de Privacyrichtlijn.

**Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: 22  
(...)]

#### *Beoordeling*

WhatsApp, met hoofdvestiging in Californië, de Verenigde Staten, bepaalt de doeleinden van en de middelen voor de verwerking van persoonsgegevens in het kader van de app.<sup>75</sup> WhatsApp is daarom de verantwoordelijke voor de verwerking van persoonsgegevens in het kader van de app.

### 3.4 Vertegenwoordiger in Nederland

#### *Uitwerking van het wettelijk kader*

Op grond van artikel 4, derde lid, van de Wbp<sup>76</sup> is het een verantwoordelijke zonder vestiging in de EU verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van de Wbp. Dit artikel eist van verantwoordelijken buiten de EU dat zij een vertegenwoordiger aanwijzen in Nederland die daardoor op Nederlands territorium aansprakelijk is voor de naleving van de wet.<sup>77</sup> Voor de toepassing van de Wbp en de daarop berustende bepalingen, wordt de vertegenwoordiger aangemerkt als de verantwoordelijke (artikel 4, derde lid, tweede volzin, van de Wbp).

#### *Beoordeling*

WhatsApp heeft verklaard dat zij geen vestiging heeft in Europa en dat zij geen vertegenwoordiger in Nederland heeft aangewezen. In reactie op het rapport Voorlopige Bevindingen heeft WhatsApp aangegeven op korte termijn een vertegenwoordiger in Nederland te willen aanstellen, maar deze aanwijzing heeft (nog) niet plaatsgehad. De zienswijze van WhatsApp leidt daarom op dit punt niet tot aanpassing van de conclusies in het rapport. Hierdoor handelt WhatsApp nog steeds in strijd met artikel 4, derde lid, van de Wbp.

### 3.5 Verwerking van persoonsgegevens

#### *Uitwerking van het wettelijk kader*

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

<sup>75</sup> Zie o.a.: "This is an agreement between WhatsApp Inc., a California corporation ("WhatsApp"), the owner and operator of www.whatsapp.com (the "WhatsApp Site"), the WhatsApp software, including WhatsApp Messenger (collectively, including all content provided by WhatsApp through WhatsApp Messenger and the WhatsApp Site, the "WhatsApp Service", or the "Service"), and you ("you" or "You"), a user of the Service." En: "This Privacy Policy is part of WhatsApp's Terms of Service and covers the treatment of user information, including personally identifying information, obtained by WhatsApp, including information obtained when you access the WhatsApp's Site, use the WhatsApp Service or any other software provided by WhatsApp." URL: <http://www.whatsapp.com/legal/?l=nl>.

<sup>76</sup> Dit artikel vormt een implementatie van artikel 4, tweede lid, van de Privacyrichtlijn.

<sup>77</sup> Zie *Kamerstukken II 1997/98*, 25 892, nr. 3, p. 76: "De naleving van de wettelijke regels met betrekking tot de van buiten de Unie verrichte verwerking van persoonsgegevens op Nederlands territorium." Zie ook WP29 Advies 8/2010 over toepasselijk recht, p. 23.



‘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>78</sup>

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.”*

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd.<sup>79</sup>

Gegevens zijn persoonsgegevens als ze naar hun aard betrekking<sup>80</sup> hebben op een persoon, zoals feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen of - gezien de context<sup>81</sup> waarin ze worden verwerkt - medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.<sup>82</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>83</sup> Ook gegevens die niet direct betrekking hebben op een

---

<sup>78</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*”.

<sup>79</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.

<sup>80</sup> Zie WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 10-11 en 25. URL:

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf): “*Er is sprake van informatie “betreffende” een persoon wanneer het gaat om informatie “over” die persoon*”, met andere woorden, de inhoud. Idem, p. 10.

<sup>81</sup> Vgl. idem, p. 10: 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>82</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>83</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 46 Zie ook idem, p. 47: “*(...) 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*

bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen over een bepaalde persoon informatie verschaffen en zijn in dat geval persoonsgegevens.<sup>84</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>85</sup> - redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.<sup>86</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>87</sup> Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke.<sup>88</sup> In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.<sup>89</sup>

### *Beoordeling*

Het CBP heeft in paragrafen 2.1 t/m 2.5 van dit rapport vastgesteld dat WhatsApp in verschillende apparatuur en systemen ten minste de volgende combinaties van gegevens van/over whatsapp-gebruikers verwerkt (heeft):

- mobiel telefoonnummer (MSISDN), inclusief land- en netwerkcode
- IMSI (uniek klantnummer)
- (gehasht) IMEI (uniek toestelnummer)
- (gehasht) MAC-adres van de iPhone (ingeval van whatsapp-gebruikers met een iPhone)

---

*worden gebruikt*", (onderstreping toegevoegd door het CBP).

<sup>84</sup> Idem, p. 46-47.

<sup>85</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, 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>86</sup> Idem, p. 47-49. In de wetsgeschiedenis bij de Wbp wordt over het begrip 'onevenredige inspanning' opgemerkt: "Dit doet zich bijvoorbeeld voor indien identificatie van personen door de computer vele dagen in beslag zou nemen." *Kamerstukken II 1998/99, 25 892, nr. 13, p. 2.*

<sup>87</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 48. Daarbij moet rekening worden gehouden met alle relevante factoren, zoals de kosten van identificatie, het beoogde doel van de verwerking, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico op organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen. WP29 136. Advies 4/2007 over het begrip persoonsgegeven van 20 juni 2007, p. 15.*

<sup>88</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 48-49.*

<sup>89</sup> Idem, p. 49.

**Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: 25  
(...)]

15 januari 2013

- 'betalingsgegevens', zoals het accounttype (gratis proef- of betaald account), het mobiele telefoonnummer en de einddatum van het gratis proef- of betaald account
- inhoud van SMS- en MMS-berichten, waaronder het ID voor push berichten: de naam die whatsapp-gebruikers hebben ingesteld voor push berichten (ingeval van whatsapp-gebruikers met een iPhone of Windows Phone) en de profielnaam (indien en voor zover whatsapp-gebruikers een profielnaam hebben opgegeven)
- (persoonlijke) statusberichten.

Daarnaast verwerkt WhatsApp het mobiele telefoonnummer (inclusief land- en netwerkcode) van niet-gebruikers van de app-diensten wanneer dat is opgenomen in het adresboek van whatsapp-gebruikers (hierna afzonderlijk of gezamenlijk genoemd: betrokkenen).

Het CBP heeft in paragrafen 2.1 t/m 2.5 van dit rapport vastgesteld dat WhatsApp de hierboven genoemde gegevens verzamelt/geneert via (gebruik van) de app die is geïnstalleerd op de smartphones van whatsapp-gebruikers. Met uitzondering van de inhoud van succesvol afgeleverde berichten en statusberichten legt WhatsApp bovengenoemde gegevens ook vast op individueel persoonsniveau en bewaart ze gedurende minimaal dertig dagen tot een jaar.

#### **Informatie 'betreffende' een natuurlijke persoon**

Als voorbeeld van persoonsgegevens die niet direct betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces wordt in de wetsgeschiedenis bij de Wbp genoemd het telefoonnummer (hier: het MSISDN, inclusief land- en netwerkcode).<sup>90</sup>

Het mobiele telefoonnummer, het unieke IMSI-klantnummer en bij bestaande gebruikers van de app totdat zij overgaan op de nieuwe wachtwoordbeveiling het (gehashte) unieke IMEI-toestelnummer dan wel het (gehashte) MAC-adres van de iPhone (unieke klant- en apparaatidentifiers) in combinatie met de inhoudelijke communicatiegegevens uit verzonden en ontvangen berichten en statusberichten, inclusief (indien en voor zover opgegeven) het push ID en de profielnaam van een whatsapp-gebruiker, en/of (technische) gegevens over het gebruik van de app zijn

---

<sup>90</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.

naar hun aard ook gegevens over gedragingen van een natuurlijke persoon (informatie over communicatiegedrag via de app).<sup>91</sup>

Verder kan het app-gebruik van een whatsapp-gebruiker een indicatie zijn voor bijvoorbeeld zijn interesses, sociale achtergrond, inkomen of gezinssamenstelling. Dergelijke informatie kan worden gebruikt voor (direct) marketing- en profileringsdoeleinden.<sup>92</sup> Niet doorslaggevend is of WhatsApp de bedoeling heeft om de gegevens 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>93</sup> en die mogelijkheid is aanwezig. WhatsApp beschikt, zoals aangegeven, bijvoorbeeld over (gegevens over) verzonden en ontvangen berichten, (technische) gegevens over het gebruik van de app en contactgegevens (waaronder het mobiele telefoonnummer).

### **Identificeerbaarheid van de persoon**

De gegevens zijn voor WhatsApp aan elkaar te koppelen en direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (whatsapp-gebruiker of niet-gebruiker van haar app-diensten).

Ten aanzien van whatsapp-gebruikers beschikt WhatsApp over ten minste het mobiele telefoonnummer. Ook ten aanzien van niet-gebruikers van haar app-diensten beschikt WhatsApp bij synchronisatie van de telefoonnummers uit de adresboeken van gebruikers over het mobiele telefoonnummer. Het mobiele telefoonnummer is een persoonsgegeven, omdat het een direct contactgegeven is, waarmee eenieder een persoon direct of indirect, via tussenstappen, kan identificeren.

Daarnaast beschikt WhatsApp over het unieke IMSI-klantnummer, het (gehashte) unieke IMEI-toestelnummer dan wel het (gehashte) MAC-adres van de iPhone van whatsapp-gebruikers. WhatsApp kan de gegevens, zonder onevenredige inspanning, aan elkaar koppelen of zo nodig via tussenstappen herleiden naar de betrokkenen (zie over de herleidbaarheid van het (gehashte) IMEI en MAC-adres verder paragraaf 3.9).

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29 Werkgroep over het begrip persoonsgegeven is hierover opgemerkt: *“(…) dat hoewel identificatie door middel van de naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan de geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakings-*

---

<sup>91</sup> Hieruit volgt informatie over het communicatiegedrag van de betrokkene en soms ook de inhoud van de communicatie.

<sup>92</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.cbpweb.nl/Pages/pv\\_20110913\\_google.aspx](http://www.cbpweb.nl/Pages/pv_20110913_google.aspx).

<sup>93</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.

*instrumenten 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>94</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>95</sup>

### **Hashing**

Hashen kan op verschillende wijzen worden toegepast. Hashen wordt bijvoorbeeld gebruikt voor het beveiligen van wachtwoorden die zijn opgeslagen in een database. De juistheid van een ingevoerd wachtwoord kan worden gecontroleerd door de hashwaarde van de invoer te vergelijken met de hashwaarde van het wachtwoord zoals die reeds in de database is opgeslagen. Voor zo'n controle hoeft men het wachtwoord zelf niet te kennen. In bepaalde gevallen en onder bepaalde voorwaarden kan het hashen van persoonsgegevens, in combinatie met andere maatregelen en waarborgen, leiden tot anonimiseren.<sup>96</sup> Of sprake is van anonimiseren hangt sterk af van de concrete omstandigheden van het geval: Van anonimiseren door middel van onder andere hashen is in elk geval geen sprake als op basis van een hash de originele waarde is te achterhalen, bijvoorbeeld als de hash kan worden teruggerekend tot het oorspronkelijke (identificerende) gegeven of opnieuw kan worden berekend. Dit is bijvoorbeeld het geval als de verantwoordelijke de beschikking heeft over de hashing formule en het oorspronkelijke gegeven.

In haar zienswijze (inclusief daaropvolgende e-mailcorrespondentie en de conference call van 4 januari 2013) stelt WhatsApp zich op het standpunt dat 'out-of-network' telefoonnummers op de whatsapp servers worden geanonimiseerd en gehasht op een manier die het extreem moeilijk maakt voor WhatsApp (of derden) om de originele telefoonnummers te achterhalen.<sup>97</sup> Het CBP heeft in paragraaf 2.2 van dit rapport vastgesteld dat WhatsApp kan beschikken over de hashing formule [VERTROUWELIJK: (...)] en het oorspronkelijke gegeven. WhatsApp kan de gehashte 'out-of-network' nummers daardoor zonder onevenredige inspanning opnieuw berekenen en bijvoorbeeld een opzoektabel maken van alle 'out-of-network' nummers in leesbare (*plain text*) en gehashte vorm. Van anonimiseren door middel van onder andere hashen is daarom geen sprake. Datzelfde geldt voor het gehashte unieke IMEI-toestelnummer dan wel het gehashte MAC-adres van de iPhone van whatsapp-gebruikers. De zienswijze van WhatsApp leidt daarom op dit punt niet tot aanpassing

<sup>94</sup> WP29 136. Advies 4/2007 over het begrip persoonsgegevens van 20 juni 2007, p. 14.

<sup>95</sup> HvJ EG 6 november 2003, zaak C-101/01 (*Lindqvist*), r.o. 27.

<sup>96</sup> Hashen kan in dat verband bijvoorbeeld meerwaarde hebben als *tussenstap* in een anonimiseringsproces.

<sup>97</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

van de conclusies in het rapport dat ook de gehashte gegevens herleidbaar zijn naar identificeerbare natuurlijke personen.

De gegevens die WhatsApp verwerkt zijn gelet op het voorgaande persoonsgegevens in de zin van artikel 1, onder a, Wbp.

### 3.6 Grondslag

#### 3.6.1 Verwerking van gegevens van niet-gebruikers uit het adresboek van whatsapp-gebruikers

*Uitwerking van het wettelijk kader*

Voor het verwerken van persoonsgegevens is een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8, aanhef en onder a tot en met f, van de Wbp.<sup>98</sup>

Artikel 8, aanhef en onder a 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;*

*(...)*

*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.*

Ten aanzien van het plaatsen en uitlezen van gegevens op apparaten van gebruikers geldt dat artikel 5, derde lid, van de e-Privacyrichtlijn (geïmplementeerd in artikel 11.7a van de Tw (nieuw)<sup>99</sup> dat in werking is getreden op 5 juni 2012)<sup>100</sup> een nadere begrenzing/inperking geeft van de toegestane verwerkingen/de grondslagen als opgesomd in artikel 8 van de Wbp die mogelijk in aanmerking kunnen komen.

Artikel 11.7a, eerste lid, van de Tw (nieuw) luidt: *Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker:*

*a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en*

*b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling.*

<sup>98</sup> Dit artikel vormt een implementatie van artikel 7, aanhef en onder a tot en met f, van de Privacyrichtlijn.

<sup>99</sup> In de wetgeschiedenis bij de Tw is opgemerkt over de reikwijdte van deze bepaling: *“Omdat de bepaling tot doel heeft om gebruikers te beschermen, geldt deze bepaling voor een ieder die gegevens wil plaatsen op randapparatuur van gebruikers in Nederland, of op die apparatuur opgeslagen gegevens wil lezen, ongeacht waar deze partij gevestigd is.” Kamerstukken I 2011/12, 32 549, E, p. 7.*

<sup>100</sup> Artikel VII, eerste lid, van het Besluit implementatie herziene telecommunicatierichtlijnen (*Stb.* 2012, 236).

Het bepaalde in het eerste lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is (artikel 11.7a, derde lid, van de Tw (nieuw), voor zover voor dit onderzoek van belang).

Toestemming van een gebruiker is gedefinieerd in artikel 11.1, aanhef en onder g, van de Tw en omvat toestemming in de zin van artikel 1, aanhef en onder i, van de Wbp.

Van toestemming in de zin van artikel 1, aanhef en onder i, van de Wbp is slechts sprake indien deze 'vrij', 'specifiek' en 'geïnformeerd' is. 'Vrij' betekent dat de betrokkene in vrijheid zijn wil moet kunnen uiten.<sup>101</sup> 'Specifiek' betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).<sup>102</sup> 'Geïnformeerd' betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.<sup>103</sup>

'Ondubbelzinnige toestemming' 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>104</sup>

#### *Beoordeling*

Het CBP heeft bij het digitaal onderzoek naar de app vastgesteld dat WhatsApp tijdens het installatieproces om lees- en schrijftoegang vraagt tot het adresboek van de gebruiker (zie paragraaf 2.1 van dit rapport). Wanneer de gebruiker de app heeft geïnstalleerd (behalve als een gebruiker met de laatste app versie op een iPhone met het besturingssysteem iOS 6 de toegang tot zijn adresboek heeft geweigerd), leest WhatsApp de mobiele telefoonnummers in zijn adresboek uit, waaronder die van niet-gebruikers. WhatsApp gebruikt deze gegevens, legt ze vast en bewaart ze om gebruikers in staat te stellen met elkaar te whatsappen, dat wil zeggen: om de gebruiker te tonen welke van zijn contacten whatsapp (zijn gaan) gebruiken.

Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat de mobiele telefoonnummers van niet-gebruikers die worden uitgelezen uit het adresboek van

<sup>101</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.

<sup>102</sup> Idem. In de opinie van de Artikel 29 Werkgroep over de definitie van "toestemming" is daarover opgemerkt: *"Een algemene toestemming zonder dat precies is aangegeven wat het doel is van de verwerking waarmee de betrokkene instemt, voldoet niet aan dit vereiste. Dat betekent dat de informatie over het doel van de verwerking niet in de algemene voorwaarden moet worden opgenomen, maar in een aparte toestemmingsclausule."* WP29 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 34-35. URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf).

<sup>103</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.

<sup>104</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.

whatsapp-gebruikers persoonsgegevens zijn. Voor deze verwerking van persoonsgegevens van niet-gebruikers is - naast toestemming als bedoeld in artikel 11.7a, eerste lid, van de Tw (nieuw) jo. artikel 1, aanhef en onder i, van de Wbp voor het uitlezen en plaatsen van gegevens op de smartphone van de gebruiker<sup>105</sup> – ook een grondslag vereist als opgesomd in artikel 8 van de Wbp.

WhatsApp heeft niet verklaard en uit het onderzoek is ook niet gebleken dat zij de gegevensverwerking voor dit doeleinde baseert op een van de grondslagen als genoemd in artikel 8, aanhef en onder b tot en met f, van de Wbp.

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

Het verschil tussen ‘toestemming’ en ‘ondubbelzinnige toestemming’ is dat bij de verantwoordelijke in het laatste geval elke twijfel moet zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven.<sup>106</sup> Gelet op de overlap van deze definities correspondeert het toestemmingsvereiste uit artikel 11.7a van de Tw (nieuw) jo. artikel 1, aanhef en onder i, van de Wbp op dit punt met de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp). De omstandigheid dat de (Europese) wetgever het nodig heeft geacht om voor het uitlezen en plaatsen van gegevens toestemming te eisen van de *gebruiker*, betekent in het licht van het voorgaande dat indien daarmee persoonsgegevens worden verwerkt (hier: mobiele telefoonnummers van niet-gebruikers uit het adresboek op de smartphone van whatsapp-gebruikers) voor deze verwerking van persoonsgegevens in beginsel alleen de grondslag in aanmerking komt als bedoeld in artikel 8, aanhef en onder a, van de Wbp, te weten: ondubbelzinnige toestemming van de *betrokkene*.

De betrokkene is degene over wie de gegevens informatie bevatten (artikel 1, aanhef en onder f, van de Wbp).

In de praktijk kan het voorkomen dat een gegeven op meerdere personen tegelijk betrekking heeft. Elk is dan betrokkene voor zichzelf en derde ten opzichte van de anderen.<sup>107</sup> De mobiele telefoonnummers van niet-gebruikers bevatten (in elk geval) informatie over henzelf. Gelet daarop zijn zij betrokkenen voor deze verwerking van persoonsgegevens. Whatsapp-gebruikers kunnen geen (ondubbelzinnige) toestemming geven namens de niet-gebruikers in hun adresboek om de hen betreffende contactgegevens door WhatsApp te laten verwerken, zonder daartoe door de betrokken niet-gebruikers te zijn gevolmachtigd. Alleen de betrokken niet-gebruikers zelf (of hun wettelijk vertegenwoordigers) kunnen dergelijke toestemming geven.

---

<sup>105</sup> Het betreft niet de technische opslag of toegang tot gegevens met als uitsluitend doel de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren, terwijl de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is (zie ook paragraaf 3.7 van dit rapport). Vgl. WP29 194. Advies 4/2012 over Cookie Consent Exemption van 7 juni 2012. URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf).

<sup>106</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 80.

<sup>107</sup> *Idem*, p. 63.



Doordat WhatsApp geen ondubbelzinnige toestemming verkrijgt van niet-gebruikers in het adresboek van whatsapp-gebruikers voor de verwerking van hun persoonsgegevens en zij deze toch verwerkt, en WhatsApp ook geen andere grondslag heeft voor deze gegevensverwerking, handelt WhatsApp in strijd met artikel 8 van de Wbp.

Het kan zijn dat WhatsApp eerst enkele met het uitlezen samenhangende verwerkingshandelingen moet verrichten om te beoordelen of de houders van de mobiele telefoonnummers in het adresboek van whatsapp-gebruikers al dan niet hun ondubbelzinnige toestemming hebben gegeven voor de gegevensverwerking: oftewel, om na te gaan of zij een grondslag heeft voor de verwerking van hun persoonsgegevens.

Voor die initiële verwerking (kortstondige leestoegang tot het volledige adresboek van een whatsapp-gebruiker) kan er - naast het vereiste van ondubbelzinnige toestemming van de betrokkenen - een afzonderlijke grondslag zijn, mits WhatsApp deze toegang alleen gebruikt om de gebruiker te helpen zijn contactpersonen te identificeren die al whatsapp-gebruiker zijn, en die in het verleden dus al ondubbelzinnige toestemming hebben gegeven aan WhatsApp om hun mobiele telefoonnummer te verzamelen en voor dit doeleinde te verwerken. Voor deze verwerking, een *compare and forget*, kan WhatsApp een grondslag hebben in artikel 8, aanhef en onder f, van de Wbp, de noodzaak voor WhatsApp om de bepalingen van de Wbp na te (kunnen) leven. De mobiele telefoonnummers van niet-gebruikers mogen in dat geval slechts worden *meeverzameld* en -gebruikt voor het strikt beperkte doel van verificatie of zij hun ondubbelzinnige toestemming hebben gegeven voor de gegevensverwerking en dienen daarna onmiddellijk te worden gewist.

In haar zienswijze (inclusief daaropvolgende e-mailcorrespondentie) stelt WhatsApp zich op het standpunt dat 'out-of-network' telefoonnummers (nummers van niet-gebruikers van de app) op de whatsapp servers worden geanonimiseerd en gehasht op een manier die het extreem moeilijk maakt voor WhatsApp (of derden) om de originele telefoonnummers te achterhalen. Volgens WhatsApp is daarom in zoverre (al) sprake van een *compare and forget* systeem.<sup>108</sup>

Het CBP heeft in paragraaf 2.2 van dit rapport vastgesteld dat de mobiele telefoonnummers van niet-gebruikers niet onmiddellijk worden gewist nadat is geverifieerd of zij hun ondubbelzinnige toestemming hebben gegeven voor de gegevensverwerking. De 'out-of-network' nummers worden gehasht en vervolgens opgeslagen en bewaard [VERTROUWELIJK: (...)].<sup>109</sup> Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat van anonimiseren door middel van hashen (ook) geen sprake is, nu WhatsApp de gehashte 'out-of-network' nummers opnieuw kan berekenen en bijvoorbeeld een opzoektabel kan maken van alle 'out-of-network' nummers in leesbare (plain text) en gehashte vorm. Er is dus geen sprake van een

<sup>108</sup> Zienswijze WhatsApp van 29 november 2012, p. 1.

<sup>109</sup> Verklaring WhatsApp tijdens de conference call van 4 januari 2013. Zie ook e-mail OPC aan WhatsApp van 4 januari 2013.

compare and forget. De zienswijze van WhatsApp leidt daarom op dit punt niet tot aanpassing van de conclusies in het rapport dat WhatsApp geen grondslag heeft voor deze gegevensverwerking.

### 3.6.2 Statusberichten

Het CBP heeft in paragraaf 2.5 van dit rapport vastgesteld dat iedere whatsapp-gebruiker statusberichten kan lezen van andere whatsapp-gebruikers, ook van onbekenden van wie hij het mobiele telefoonnummer in zijn adresboek heeft.<sup>110</sup>

Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat statusberichten, in combinatie met het mobiele telefoonnummer en overige klant- en apparaatidentifiers, persoonsgegevens zijn.

Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp de informatie over statusberichten aan haar gebruikers uitgebreid.

De standaardinstelling voor statusberichten is: *"Hey there! I am using WhatsApp"*. Een gebruiker kan dit bericht wijzigen via het menu van de app. Als de gebruiker het bericht zelf wijzigt, en desgewenst een eigen tekst invoert, kan uit zijn handeling in dit specifieke geval in beginsel toestemming worden afgeleid voor de verwerking ervan.<sup>111</sup>

De OPC benadrukt in haar voorlopige bevindingen dat WhatsApp extra waarborgen moet inbouwen tegen de risico's van de brede verspreiding van potentieel gevoelige informatie opgenomen in statusberichten (bijvoorbeeld de exacte locatie waar de gebruiker verblijft, of mededelingen over zijn gezondheid). Hoewel er volgens het CBP op basis van het beschikbare onderzoeksmateriaal formeel geen overtreding van de Wbp lijkt te zijn, onderschrijft het CBP de aanbeveling van de OPC dat whatsapp-gebruikers een waarschuwing moeten krijgen over de brede verspreiding van het bericht, telkens als zij hun statusbericht aanpassen (als *best practice*). WhatsApp geeft in haar zienswijze aan dat het toevoegen van een waarschuwing/pop-up over de verspreiding van statusberichten - als gebruikers hun statusbericht aanpassen - op de agenda voor productontwikkeling staat. De zienswijze van WhatsApp leidt op dit punt niet tot aanpassing van de aanbeveling in het rapport.

---

<sup>110</sup> In de Terms of Service en Privacy Notice wordt hierover vermeld: *"Submissions may be globally viewed by users that have your mobile phone number, so don't submit or post status messages or profile photos that you don't want to be seen globally. A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service."*

<sup>111</sup> Vgl. o.a. *Handleiding voor verwerkers van persoonsgegevens*. Wet bescherming persoonsgegevens, Ministerie van Justitie, Den Haag: 2002, p. 21-22. URL: <http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html>.

### 3.7 Bovenmatigheid: toegang tot het adresboek op de smartphone

#### *Uitwerking van het wettelijk kader*

Artikel 11, eerste lid, van de Wbp, bepaalt, voor zover voor dit onderzoek van belang: *Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.*<sup>112</sup>

Het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, is bepalend voor de hoeveelheid en de soort gegevens die onderwerp van verwerking vormen. De gegevens dienen met het oog op dat doel niet bovenmatig (overbodig/overvloedig) te zijn.<sup>113</sup>

#### *Beoordeling*

Het CBP heeft bij het digitaal onderzoek naar de app vastgesteld dat het voor een gebruiker niet mogelijk was en is (behalve in de laatste app versie op een iPhone met besturingssysteem iOS versie 6) om het installatieproces (volledig) te doorlopen zonder WhatsApp toegang te verlenen tot de mobiele telefoonnummers van alle andere whatsapp-gebruikers en niet-gebruikers in zijn adresboek (zie paragraaf 2.2 van dit rapport).

Om gebruikers in staat te stellen met elkaar te whatsappen, is het niet nodig voor WhatsApp om alle mobiele telefoonnummers uit hun adresboek te verzamelen, te gebruiken, vast te leggen en te bewaren. Een gebruiker moet zeggenschap hebben of hij de telefoonnummers van zijn contacten ter beschikking wil stellen van WhatsApp, en zo ja, welke contacten. Hij wil misschien maar met een of twee andere gebruikers communiceren via whatsapp, en niet met alle contacten uit zijn adresboek.

In haar zienswijze wijst WhatsApp erop dat gebruikers in de laatste iOS versie van de app (volgens WhatsApp het meest gebruikte besturingssysteem voor de app) de mogelijkheid hebben om WhatsApp geen toegang te geven tot hun elektronische adresboek. Als zij via een dialoogbox opgeroepen door het besturingssysteem de toegang weigeren, kunnen zij handmatig een telefoonnummer invoeren om die persoon een whatsapp-bericht te versturen.<sup>114</sup>

Doordat WhatsApp gebruikers niet de keuzemogelijkheid bood en biedt (behalve in de laatste app versie op een iPhone met besturingssysteem iOS versie 6) om de app te gebruiken zonder toegang te verlenen tot het adresboek, of louter toegang te verlenen tot geselecteerde contactpersonen waarmee zij (op dat moment) willen whatsappen,<sup>115</sup> was respectievelijk is een groot deel van de uit het adresboek

<sup>112</sup> Dit artikel vormt een implementatie van artikel 6, eerste lid, onder c, van de Privacyrichtlijn.

<sup>113</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 96.

<sup>114</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

<sup>115</sup> WhatsApp moet, gelet op de reeds bestaande mogelijkheid voor whatsapp-gebruikers om zelf nieuwe contacten uit te nodigen en de mogelijkheid om de app te installeren en te gebruiken zonder toegang tot het adresboek in de laatste app versie op een iPhone met **Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: 34 (...)]

verzamelde mobiele telefoonnummers bovenmatig. Hierdoor handelde en handelt WhatsApp in strijd met artikel 11, eerste lid, van de Wbp. Doordat WhatsApp ten aanzien van de gegevensverwerking via de laatste app versie op een iPhone met besturingssysteem iOS versie 6 gebruikers de mogelijkheid geeft om de app te installeren en gebruiken zonder toegang tot het adresboek handelt WhatsApp op dat punt niet langer in strijd met artikel 11, eerste lid, van de Wbp. De zienswijze van WhatsApp leidt in zoverre tot aanpassing van de conclusies in het rapport. Ten aanzien van andere besturingssystemen leidt de zienswijze van WhatsApp op dit punt niet tot aanpassing van de conclusies in het rapport.

### 3.8 Bewaartermijn gegevens van whatsapp-gebruikers

#### *Uitwerking van het wettelijk kader*

Artikel 10, eerste lid, van de Wbp bepaalt dat persoonsgegevens niet langer mogen worden bewaard *in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervoelgens worden verwerkt.*<sup>116</sup>

Soms is in bijzondere wetgeving de algemene termijn dat gegevens kunnen worden bewaard, gefixeerd. Anders dient de verantwoordelijke zich af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. Zijn die termijnen verlopen dan zal hij de gegevens niet meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel.<sup>117</sup>

#### *Beoordeling*

Het CBP heeft in paragraaf 2.3 van dit rapport vastgesteld dat WhatsApp gegevens van gebruikers gedurende een jaar bewaart nadat ze hun account voor het laatst hebben gebruikt. Dit kan oplopen tot een bewaartermijn van twee jaar als een betrokkene de app heeft geïnstalleerd en slechts een keer heeft uitgeprobeerd, maar het account niet actief heeft opgeheven. Het betreft het mobiele telefoonnummer, het accounttype en de beëindigingsdatum van de afgenomen dienst.

Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat deze gegevens persoonsgegevens zijn.

Er is in bijzondere wetgeving geen vaste minimumbewaartermijn vastgesteld ten aanzien van deze persoonsgegevens.

De huidige door WhatsApp zelf bepaalde bewaartermijn ten aanzien van inactieve gebruikers betekent dat op andere smartphones dan de iPhone gegevens tot twee jaar lang (kunnen) worden bewaard, als een gebruiker (eenmalig) gratis whatsapp

---

besturingssysteem iOS versie 6 (zie paragraaf 2.2 van dit rapport), technisch ook in staat worden geacht om een technisch alternatief te programmeren.

<sup>116</sup> Dit artikel vormt een implementatie van artikel 6, eerste lid, onder e, van de Privacyrichtlijn.

<sup>117</sup> *Kamerstukken II 1997/98, 25 892, nr. 3, p. 95.*

installeert en uitprobeert en er vervolgens geen gebruik meer van maakt (voor de iPhone is er geen subscription periode van een jaar). Voor deze lange bewaartermijn bestaat geen noodzaak ten aanzien van inactieve gebruikers. Zij kunnen immers na afloop van de gratis proefperiode/(betaalde) subscription periode de app niet meer gebruiken zonder daar (opnieuw) voor te betalen. Dit ontbreken van een noodzaak geldt temeer omdat er andere, minder ingrijpende manieren bestaan om gegevens van inactieve gebruikers op te schonen. Een veelgebruikte methode is het sturen van een of meerdere herinneringen aan inactieve gebruikers. WhatsApp kan met haar gebruikers communiceren. Na het uitblijven van een reactie van de gebruiker kan het account automatisch worden opgeheven, en de gegevens vernietigd.

Volgens WhatsApp moet zij, met name als het om een betaald account gaat, de gegevens bewaren gedurende de *subscription* periode voor een goede dienstverlening zonder kwaliteitsverlies (tenzij het gaat om gegevens verwijderd door de gebruiker voor de vervaldatum).<sup>118</sup> Het CBP heeft hierboven gemotiveerd vastgesteld dat geen noodzaak bestaat voor het bewaren van de gegevens van inactieve gebruikers tot een jaar *na afloop* van de subscription periode (op andere smartphones dan de iPhone maximaal tot twee jaar lang). De zienswijze van WhatsApp leidt op dit punt daarom niet tot aanpassing van de conclusies in het rapport. Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp aangekondigd dat bewaartermijnen en de informatie daarover op de agenda voor productontwikkeling staan, maar geen termijnen genoemd.

De noodzaak om gegevens van inactieve whatsapp-gebruikers zo lang te bewaren als WhatsApp nu doet, is gelet op het voorgaande niet aangetoond. Hierdoor handelt WhatsApp in strijd met artikel 10, eerste lid, van de Wbp.

### 3.9 Beveiliging

#### *Uitwerking van het wettelijk kader*

Ingevolge artikel 13 van de Wbp dient de verantwoordelijke *passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.*<sup>119</sup>

De beveiligingsverplichting uit dit artikel strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.<sup>120</sup>

Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de allerswaarste beveiliging te nemen. Er moet sprake zijn van

<sup>118</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

<sup>119</sup> Dit artikel vormt een implementatie van artikel 17, eerste lid, van de Privacyrichtlijn.

<sup>120</sup> *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98.

een adequate beveiliging. Technische en organisatorische maatregelen dienen cumulatief te worden getroffen (waaronder bijvoorbeeld beveiliging met een password en door middel van encryptie).<sup>121</sup>

Onder 'onrechtmatige vormen van verwerking' vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan.<sup>122</sup>

#### *Beoordeling*

Het CBP heeft in paragraaf 2.4.1 van dit rapport vastgesteld dat WhatsApp bij aanvang van het onderzoek wachtwoorden genereerde door gebruik te maken van het WiFi MAC-adres op iPhones, en van het unieke IMEI-toestelnummer op andere typen smartphones.

Aan het gebruik van het interne WiFi MAC-adres van smartphones zijn grote beveiligingsrisico's verbonden. Een whatsapp-gebruiker die verbonden is met een WiFi-verbinding maakt hierbij gebruik van het WiFi MAC-adres van de smartphone. De smartphone zendt dit MAC-adres voortdurend in leesbare vorm uit, zelfs als het een beveiligde verbinding betreft. Iedereen die in het bereik is van dit WiFi netwerk kan het MAC adres vervolgens met vrij verkrijgbare (gratis) netwerkanalyse software opvangen. Iedereen kan daarna het wachtwoord namaken.<sup>123</sup>

Ook zonder de netwerkanalyse software is het MAC-adres gemakkelijk te achterhalen. Iedereen die op hetzelfde WiFi netwerk zit, kan het MAC-adres opzoeken van elk ander apparaat in dit netwerk in de opzoeklijst voor MAC-adressen.<sup>124</sup>

Ook aan het maken van een wachtwoord met gebruik van het IMEI zijn beveiligingsrisico's verbonden. Het is mogelijk, gezien de huidige stand van de techniek [VERTROUWELIJK: (...)], om een opzoektabel te maken van alle mogelijke IMEI-nummers met bijbehorende hashwaarde. Het is aannemelijk dat de rekenkracht van grafische processoren (GPU) in de toekomst verder toeneemt. Op dit moment zijn opzoektabellen met een lengte van twaalf cijfers vrij voorhanden op internet. Het is voorzienbaar dat er in de nabije toekomst ook opzoektabellen beschikbaar komen met een lengte van vijftien cijfers, dat wil zeggen, de lengte van het IMEI.<sup>125</sup>

Daarnaast wordt [VERTROUWELIJK: (...)] afgeraden door [VERTROUWELIJK: (...)] in verband met het risico op *hash collisions*. Dat wil zeggen dat verschillende IMEI-nummers tot dezelfde hashwaarde kunnen leiden. Een verder risico ten aanzien van het IMEI-nummer is dat andere apps dit nummer ook kunnen verzamelen en verwerken.<sup>126</sup> De verwerking gebeurt vaak in leesbare vorm, zodat iedereen die in het bereik is van het WiFi netwerk het IMEI-nummer met vrij verkrijgbare (gratis)

---

<sup>121</sup> Idem, p. 99.

<sup>122</sup> Idem, p. 98.

<sup>123</sup> [VERTROUWELIJK: (...)]

<sup>124</sup> Het Address Resolution Protocol (ARP) maakt gebruik van opzoeklijsten met MAC-adressen van apparaten verbonden met hetzelfde netwerk.

<sup>125</sup> [VERTROUWELIJK: (...)]

<sup>126</sup> Wall Street Journal series 'What They Know Mobile'. URL: <http://blogs.wsj.com/wtk-mobile/>.

netwerkanalyse software kan opvangen. Een ander risico is dat als een app-ontwikkelaar met een grote verzameling IMEI-nummers getroffen wordt door een datalek, de IMEI-nummers beschikbaar kunnen komen op internet en anderen dus het wachtwoord kunnen reproduceren met behulp van [VERTROUWELIJK: (...)].

De wijze waarop WhatsApp wachtwoorden aanmaakte, en het hierboven beschreven gemak waarop deze kunnen worden nagemaakt, stelde gebruikers bloot aan het reële risico dat anderen hun wachtwoord konden namaken, en daarmee namens hen berichten konden versturen en lezen.

Het CBP heeft in paragraaf 3.5 van dit rapport vastgesteld dat de berichten, in combinatie met gegevens over de verzender en/of ontvanger, persoonsgegevens zijn. Omdat whatsapp-berichten gevoelige, inhoudelijke informatie kunnen bevatten (het betreft inhoudelijke communicatie), leverde de door WhatsApp gekozen werkwijze onaanvaardbare risico's op voor de persoonlijke levenssfeer van betrokkenen.

Omdat WhatsApp geen bij de gevoeligheid van de gegevens passende technische maatregelen had getroffen bij het aanmaken van het wachtwoord, handelde WhatsApp in strijd met artikel 13 van de Wbp.

Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp haar werkwijze aangepast, in die zin dat er app updates beschikbaar zijn die niet langer het WiFi MAC-adres of het IMEI-toestelnummer gebruiken, maar [VERTROUWELIJK: (...)], aldus haar zienswijze.<sup>127</sup> Het CBP heeft in paragraaf 2.4.1 vastgesteld dat Whatsapp in december 2012 nieuwe updates van de app heeft uitgebracht, en gebruik van de nieuwste versies bij actieve gebruikers forceert. Door deze combinatie van technische en organisatorische maatregelen handelt WhatsApp ten aanzien van actieve gebruikers na de update niet langer in strijd met artikel 13 van de Wbp. De zienswijze van WhatsApp leidt in zoverre tot aanpassing van de conclusies in het rapport.

Ten aanzien van de inactieve gebruikers resteert een risico. Het CBP heeft vastgesteld dat inactieve whatsapp-gebruikers niet worden geconfronteerd met een 'gedwongen update'. WhatsApp heeft verklaard dat het remediëren van dit risico voor inactieve gebruikers op de agenda voor productontwikkeling komt te staan, maar daarbij geen termijn genoemd.<sup>128</sup> De zienswijze van WhatsApp leidt op dat punt (nog) niet tot aanpassing van de conclusies in het rapport. Doordat op dit moment WhatsApp nog niet voor alle accounts gebruik maakt van de nieuwe methode, handelt WhatsApp nog in strijd met artikel 13 van de Wbp.

Het CBP heeft in paragraaf 2.4.2 van dit rapport vastgesteld dat WhatsApp bij aanvang van het onderzoek door het CBP en de OPC de berichten via de app op onversleutelde wijze verzond. Dit leidde ertoe dat anderen de inhoud van berichten in leesbare vorm konden onderscheppen.

---

<sup>127</sup> Zienswijze WhatsApp van 29 november 2012, p. 2.

<sup>128</sup> Verklaring WhatsApp tijdens de conference call op 4 januari 2013.

Door het ontbreken van enige vorm van versleuteling van de gegevens tijdens de overdracht tussen de smartphone en de whatsapp servers, bijvoorbeeld met SSL *'end-to-end'* encryptie, een algemeen beschikbare en voor de hand liggende beveiligingsmaatregel van deze gevoelige gegevens, handelde WhatsApp in strijd met artikel 13 van de Wbp.

Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp maatregelen getroffen om de berichten versleuteld te versturen. Hierdoor is de overtreding van artikel 13 van de Wbp op dit punt inmiddels beëindigd.



## 4. CONCLUSIES

WhatsApp, gevestigd in Californië, Verenigde Staten, levert met whatsapp een dienst die toegankelijk is voor en nadrukkelijk gericht is op personen in Nederland. De app wordt door miljoenen Nederlandse gebruikers met een smartphone gebruikt.

Het CBP is bevoegd om onderzoek in stellen op grond van de Wbp omdat via de app op smartphones in Nederland persoonsgegevens worden verwerkt. Het gaat onder meer om het mobiele telefoonnummer, unieke klant- en apparaatidentifiers en (als opgegeven) het push ID en de profielnaam van whatsapp-gebruikers. Daarnaast verwerkt WhatsApp het mobiele telefoonnummer van niet-gebruikers wanneer dat is opgenomen in het adresboek van whatsapp-gebruikers. Deze gegevens zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over communicatiegedrag via de app). De gegevens zijn voor WhatsApp, bijvoorbeeld via het mobiele telefoonnummer (een direct contactgegeven), direct dan wel indirect - via tussenstappen - te herleiden tot een identificeerbare natuurlijke persoon (whatsapp-gebruiker of niet-gebruiker).

WhatsApp gebruikt smartphones van whatsapp-gebruikers - door middel van de app die op de apparaten is geïnstalleerd - als middel bij de verwerking van persoonsgegevens in het kader van de app. De Wet bescherming persoonsgegevens (Wbp) is (evenals hoofdstuk 11 van de Telecommunicatiewet; Tw) dwingend recht. Dit betekent dat de toepasselijkheid in deze kwestie daarvan niet via een eenzijdige verklaring of contractueel in de algemene voorwaarden door WhatsApp kan worden uitgesloten.

### **Toegang tot het adresboek**

Wie whatsapp wil gebruiken, moet toegang geven tot zijn volledige elektronische adresboek, inclusief de mobiele telefoonnummers van contacten die de app niet gebruiken (behalve in de laatste app versie op een iPhone met iOS 6). Doordat WhatsApp geen ondubbelzinnige toestemming verkrijgt van niet-gebruikers voor de verwerking van hun persoonsgegevens, en WhatsApp ook geen andere grondslag heeft voor deze gegevensverwerking, handelt WhatsApp in strijd met artikel 8 van de Wbp.

Om gebruikers in staat te stellen met elkaar te whatsappen, hoeft WhatsApp niet alle mobiele telefoonnummers uit hun adresboek te verwerken. Doordat WhatsApp gebruikers (behalve in de laatste app versie op een iPhone met iOS 6) niet de mogelijkheid biedt om te kiezen of zij hun contacten aan WhatsApp ter beschikking willen stellen en zo ja, welke, is een groot deel van de uit het adresboek verzamelde mobiele telefoonnummers bovenmatig. Hierdoor handelt WhatsApp in strijd met artikel 11, eerste lid, van de Wbp.

### **Bewaartermijn**

Van inactieve gebruikers bewaart WhatsApp nog gedurende een jaar persoonsgegevens. Doordat WhatsApp niet heeft aangetoond dat de gegevens van inactieve gebruikers zo lang bewaard moeten blijven, handelt WhatsApp in strijd met artikel 10, eerste lid, van de Wbp.

**Openbare versie** (Bedrijfs)vertrouwelijke passages zijn weergegeven als [VERTROUWELIJK: 40  
(...)]

15 januari 2013

## **Beveiliging**

De wijze waarop WhatsApp wachtwoorden genereerde, door gebruik te maken van het gehashte WiFi MAC-adres op iPhones, en van het gehashte IMEI-toestelnummer op andere typen smartphones, stelde whatsapp-gebruikers bloot aan het risico dat anderen hun wachtwoord konden namaken, en daarmee namens hen berichten konden versturen en lezen. Hierdoor handelde WhatsApp in strijd met artikel 13 van de Wbp. Naar aanleiding van het rapport Voorlopige Bevindingen heeft WhatsApp haar werkwijze aangepast, en een nieuwe methode gekozen om wachtwoorden aan te maken. WhatsApp heeft in december 2012 nieuwe versies van de app uitgebracht, en dwingt technisch af dat actieve gebruikers overschakelen naar deze nieuwste versies doordat zij de app anders niet meer kunnen gebruiken (geforceerde update). Ten aanzien van inactieve gebruikers die hun app niet updaten blijven risico's bestaan. Gebruikers krijgen immers alleen een nieuw wachtwoord toegewezen als zij *actief* een nieuwe update installeren. WhatsApp heeft aangegeven deze risico's voor inactieve gebruikers te zullen adresseren, maar heeft daarbij geen termijn genoemd. Doordat op dit moment WhatsApp niet voor alle accounts gebruik maakt van de nieuwe methode, handelt WhatsApp ten aanzien van de gebruikers met nog een wachtwoord gebaseerd op het WiFi MAC-adres of het IMEI-toestelnummer (nog) in strijd met artikel 13 van de Wbp.

Bij aanvang van het onderzoek door het CBP en de OPC verstuurde WhatsApp de berichten via de app op onversleutelde wijze. Hierdoor konden anderen de inhoud daarvan in leesbare vorm onderscheppen. Naar aanleiding van het onderzoek heeft WhatsApp versleuteling aangebracht. Hierdoor is de overtreding van artikel 13 van de Wbp op dit punt beëindigd.

## **Statusberichten**

Iedere whatsapp-gebruiker kan de statusberichten lezen van andere whatsapp-gebruikers, ook van onbekenden, van wie hij de mobiele telefoonnummers in zijn adresboek heeft. Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp de informatie over de verspreiding van statusberichten aan haar gebruikers uitgebreid. De OPC benadrukt dat WhatsApp extra waarborgen moet inbouwen tegen de risico's van de brede verspreiding van potentieel gevoelige statusinformatie. Hoewel op dit punt formeel de Wbp niet lijkt te worden overtreden, onderschrijft het CBP de aanbeveling van de OPC dat gebruikers van WhatsApp een waarschuwing moeten krijgen, telkens als zij hun statusbericht aanpassen, over de verspreiding daarvan.

## **Aangekondigde maatregelen**

Naar aanleiding van het onderzoek door het CBP en de OPC heeft WhatsApp aangekondigd dat (i) het adresseren van het restrisico in de wachtwoordbeveiliging van inactieve gebruikers, (ii) bewaartermijnen en de informatie daarover en (iii) het toevoegen van een waarschuwing/pop-up over de verspreiding van statusberichten - als gebruikers hun statusbericht aanpassen - op de agenda voor productontwikkeling staan, maar zij heeft daarbij geen termijnen genoemd.