Praktische juridische tips mobile

DDMA september 2013

Voorwoord

Mobile is niet meer weg te denken uit de maatschappij. Het is de toekomst en de marketing- en technologiesector speelt hier op in. Dagelijks verschijnen er tientallen nieuwe apps en websites worden steeds meer mobile ready gemaakt.

Ook binnen mobile spelen allerlei juridische regels zodra een app gebruik maakt van persoonsgegevens. Zo heeft bijvoorbeeld de Artikel 29-werkgroep (het samenwerkingsverband van alle privacytoezichthouders in de EU, waaronder het CBP) hier richtlijnen voor opgesteld.

Om de branche inzicht te geven in alle relevante privacywetten die van toepassing zijn voor mobile marketing in Nederland heeft DDMA, in samenwerking met de DDMA Commissie Mobile het document 'Praktische juridische tips mobile' ontwikkeld. In dit document worden onder andere de juridische aspecten van apps, pushberichten, cookies, SMS en Bluetooth besproken. Het document bevat daarnaast ook een handige checklist waarmee u kunt checken of een app voldoet aan de juridische richtlijnen.

DDMA september 2013

Leden DDMA Commissie Mobile
Ivonne Bojoh
Tim Akkerman
Patrick Loppé
Bulent Polat
Gertjan Rösken
Jeroen Verschoor

DDMA
Jitty van Doodewaerd
Monique Rutten
Henk Bultena

Inhoudsopgave

1. Welke Nederlandse wetten zijn relevant voor mobile?

Maakt uw app gebruik van persoonsgegevens? Dan zijn de volgende Nederlandse wetten van toepassing:

- Wet bescherming persoonsgegevens (Wbp)
- Telecommunicatiewet
- Burgerlijk wetboek

1.1. Wat is een persoonsgegeven?

De Wbp spreekt van een persoonsgegeven. Wat verstaan we hier eigenlijk onder? Volgens artikel 1 van de Wbp is dit:

Elk gegeven betreffende een **geïdentificeerde** of **identificeerbare natuurlijke persoon**.

Oftewel, een persoonsgegeven is een gegeven dat direct of indirect herleidbaar is tot een individu. Denk hierbij aan een naam, adres, woonplaats, telefoonnummer en e-mailadres. Smartphones en tablets bevatten veel **persoonlijke gegevens** van en over hun gebruikers. Dit zijn bijvoorbeeld contacten, locatie-informatie, creditcardinformatie, foto's, video's en login-gegevens van social media. Ook unieke nummers (identifiers als IMSI, IMEI, MAC-adres, UUID's etc) op de smarthphones en tablets zijn persoonsgegevens. Dit geldt ook voor de gegevens die in combinatie met deze identifiers verzameld worden over het gebruik van de app (bijv. locatiegegevens, surfgedrag, logingegevens, betalingen, bekeken advertenties etc.).

2. Privacy-correcte apps

De instantie die in Nederland toezicht houdt op het naleven van de Wbp is het College bescherming persoonsgegevens (CBP). Het College publiceerde in maart 2013 een opinie[1] van de Artikel 29-werkgroep (samenwerkingsverband alle privacytoezichthouders EU) hoe privacyschending via apps kan worden voorkomen. Dit hoofdstuk geeft een vertaalslag van deze opinie (gebaseerd op de Wbp) naar praktische juridische handvatten voor app-ontwikkelaars en marketeers.

2.1 Informeren over gebruik persoonsgegevens

De gebruiker moet geïnformeerd worden dat zijn persoonlijke gegevens gebruikt worden door de app. Dit moet gebeuren **voordat** de app informatie van het apparaat haalt (bijv. toegang tot het fotoalbum) of daar op plaatst (bijv. het gebruik van contactgegevens). U informeert de gebruiker op correcte wijze wanneer u **duidelijke en begrijpbare doelen** formuleert, waarvoor de gegevens worden gebruikt. Deze doelen mogen niet tussentijds gewijzigd worden zonder toestemming van de gebruiker. Een voorbeeld van een doel is het gebruik van de contactlijst om de berichtenfunctie correct te laten functioneren óf het gebruik maken van GPS-informatie om de gebruiker bepaalde locaties in de app te tonen.

2.2 Toestemming persoonsgegevens

Het installeren van een app valt onder artikel 11.7a Telecommunicatiewet, in de volksmond ook wel de cookiewet genoemd. Dit artikel geeft aan dat een gebruiker toestemming moet geven voor een app informatie mag plaatsen op of uitlezen van zijn randapparatuur. Omdat een app per definitie informatie plaatst op of leest van randapparatuur valt hij daarmee onder het toestemmingsvereiste van de cookiewet en de e-privacy richtlijn. Deze toestemming moet gegeven worden **voordat** de app informatie van het apparaat haalt of daar informatie op plaatst. De Artikel 29-werkgroep geeft

[1] http://www.cbpweb.nl/Pages/pb_20130314-wp29-opinie-mobiele-apps.aspx

aan dat in deze toestemming apart toestemming moet worden gevraagd voor de verschillende soorten categorieën gegevens waar de app toegang tot heeft (denk aan GPS en contactenlijsten van de smartphone of tablet).

Als u nu deze toestemming heeft mag u de app installeren op de smartphone. Maar mag u dan ook zomaar persoonsgegevens verzamelen? De Artikel 29-werkgroep zegt vervolgens dat voor de informatie (persoonsgegevens) die u na installatie van de app verzamelt, niet perse nogmaals toestemming hoeft te worden gevraagd. Als u de informatie bijvoorbeeld nodig hebt voor het leveren van de dienst (bijv. een routeplanner) hoeft u hiervoor niet nog eens toestemming te vragen. Dit geldt ook voor informatie die u kunt gebruiken voor marketingdoeleinden. U moet wel altijd toestemming vragen als u elektronische contactgegevens (bijv. een e-mailadres) of bijzondere persoonsgegevens (ras, geloof, ziekte e.d.) verzamelt.

2.3 Toestemming intrekken

Gebruikers van de app moeten altijd de mogelijkheid hebben de toestemming voor gebruik van hun persoonsgegevens in te trekken door:

a. Dit aan te geven in het besturingssysteem en/of in de app
b. De app te de-installeren waardoor de verzamelde persoonsgegevens worden verwijderd

2.4 Verzamel alleen wat echt nodig is

Ook is het belangrijk dat er alleen gegevens verzameld worden die echt nodig zijn voor de gewenste functionaliteit van de app of waarover u geïnformeerd heeft.

2.5 Beveiliging

U moet technische maatregelen nemen zodat de persoonlijke gegevens die gebruikt worden door de app, goed beveiligd zijn. De Artikel 29-werkgroep geeft als aanbeveling dat u gebruikers actief dient te informeren als er een datalek heeft plaatsgevonden.

2.6 Apps voor kinderen

Voor kinderen gelden naast bovengenoemde regels nog enkele belangrijke voorwaarden:

- Wanneer er persoonsgegevens worden verwerkt van een minderjarig kind (jonger dan 16 jaar) moeten de ouders van het kind hiervoor toestemming geven.
- Het is niet toegestaan om de gegevens van kinderen onder de 13 jaar te gebruiken om selecties te maken voor advertenties gericht op deze groep.
- De informatie in de app moet op een simpele manier worden aangeboden met taalgebruik dat aansluit bij de leeftijd van het kind waarop de app zich richt.

2.7 Apps uit het buitenland

Het CBP geeft aan[2] dat het niet uit maakt of de app-ontwikkelaar in Nederland gevestigd is of in het buitenland. De Nederlandse privacywet (Wbp) is van toepassing als de buitenlandse app-ontwikkelaar gebruik maakt van apparatuur in Nederland.

2.8 Privacy voorwaarden

[2] http://www.mijnprivacy.nl/Vraag/Apps/Paginas/Apps.aspx

De privacy voorwaarden van toepassing op de app moeten:

- Leesbaar en begrijpelijk zijn (de Artikel 29-werkgroep stelt iconen voor)
- Goed toegankelijk zijn voor de gebruiker (bijv. als tekst in de app of een link naar de online privacy voorwaarden)

3. Huidige situatie vs opinie Artikel 29-werkgroep

Anno 2013 zijn er twee leidende besturingssystemen: iOs (Apple) en Android (Google).
Wereldwijd volgen app-ontwikkelaars de technische richtlijnen van o.a. deze Amerikaanse technologie-partijen[3]. De vraag is of deze manier van informeren en toestemming vragen strookt met de opinie van de Artikel 29-werkgroep. In deze paragraaf zetten we de beroepspraktijk en de opinie van de toezichthouders naast elkaar.

3.1 Informeren over gebruik persoonsgegevens

Wat is de huidige situatie?

De app moet de gebruiker informeren over het gebruik van zijn persoonsgegevens en met welk doel. Dit moet gebeuren voordat de app informatie van het apparaat haalt of daar informatie op plaatst. Deze doelen mogen niet tussentijds gewijzigd worden zonder toestemming van de gebruiker.

Een app op een Androidtoestel geeft via Google Play in hun toestemmingslijst beknopte informatie over het doel van de verwerking van de persoonsgegevens. Bijvoorbeeld: *Applicatie mag alle contactgegevens (adressen) die op uw apparaat zijn opgeslagen, lezen.*

Apple formuleert de informatie over het doel van een bepaalde verwerking van een persoonsgegeven vrij algemeen. Bijvoorbeeld: *App X wil uw huidige*

[3] De opinie van het College is ook van toepassing op o.a. Blackberry, Windows en andere.

locatie gebruiken. In dit geval weet een gebruiker van de app niet precies waarom de app toegang moet hebben tot de GPS van een telefoon. Strookt dit met de opinie van de Artikel 29-werkgroep?
De vraag is of het CBP bovenstaande manieren van informeren over de verwerking van de doelen vindt voldoen aan de eisen van de Wbp. De informatie over het doel van een bepaalde verwerking van een persoonsgegeven is vrij algemeen.

Bijvoorbeeld: *de app heeft toegang nodig tot uw locatievoorziening.* In dit geval weet een gebruiker niet precies waarom de app toegang moet hebben tot de GPS van zijn smartphone of tablet. De Artikel 29-werkgroep geeft aan dat een gebruiker van een app duidelijk en begrijpelijk geïnformeerd moet worden over de doelen van de verwerking van de persoonsgegevens door een app.

De app dient de gebruiker te informeren over het doel van verwerking voordat de gebruiker van de app toestemming geeft voor het gebruik van zijn gegevens. Dit kan bijvoorbeeld vanuit de downloadomgeving. Het CBP geeft in correspondentie echter aan dat de app-bouwer in zijn interface zelf zal moeten voorzien in specifieke informatie welke gegevens door hem voor welke doel worden verwerkt als er gegevens over de lijn gaan, en hoelang de gegevens door hem worden bewaard. Dit zou technisch bijvoorbeeld inhouden dat voordat de schermmelding van toestemming geven verschijnt er met een eigen venster geïnformeerd moet worden over de verwerking van de persoonsgegevens van de app. Daarna zou er op accepteren geklikt kunnen worden. Uit de informatie moet blijken waarvoor de persoonsgegevens worden gebruikt.

De uitgebreide informatie met betrekking tot de privacy van de gebruiker – bijvoorbeeld over beveiliging en het gebruik van cookies - kan verder in het

privacy statement van de app worden verwerkt. Deze kan in de app worden opgenomen of vanuit de app gelinkt worden naar een webpagina.

3.2 Toestemming persoonsgegevens

Wat is de huidige situatie?

De Apple Store en Google Play bieden technisch de mogelijkheid toestemming te vragen aan de gebruiker voordat de app informatie van het apparaat haalt of daar informatie op plaatst.

Google Play vraagt vóór het downloaden van de app **éénmalig** toestemming voor de verschillende persoonsgegevens die de app verwerkt. Dit gebeurt door middel van een lijst met doelen die voorafgaand aan de installatie van een app wordt getoond en welke de gebruiker moet accepteren. Bijvoorbeeld: *App X heeft toegang nodig tot telefoonoproepen, systeemhulpmiddelen, netwerkcommunicatie, uw locatie, uw persoonlijke persoonsgegevens etc.* Soms wordt ook toestemming in de app zelf gevraagd als een app bijvoorbeeld voor het eerst gebruik maakt van GPS.

Apple vraagt toestemming zodra zij voor het eerst gebruik maakt van een bepaalde functionaliteit. Denk bijvoorbeeld aan een app die voor de eerste keer de locatievoorziening nodig heeft voor een digitale kaart. De gebruiker ontvangt dan de melding: *de app wil toegang tot uw huidige locatie* en kan hierop akkoord geven.

Strookt dit met de opinie van de Artikel 29-werkgroep?

De Artikel 29-werkgroep geeft in haar opinie aan dat er apart toestemming moet worden gevraagd voor het verwerken van de categorieën gegevens waar de app toegang tot heeft. Dit is bijvoorbeeld toestemming voor toegang tot GPS of toegang tot een contactenlijst. Dit moet gebeuren **voordat** de app informatie van het apparaat haalt of daar informatie op plaatst.

Praktijkvoorbeeld ‘informeren & toestemming’ o.b.v. opinie Artikel 29-Werkgroep

De gemeente Amsterdam wil haar cultureel erfgoed eenvoudig toegankelijk maken voor toeristen. Zij ontwikkelt daarom een app die interactieve looproutes door het historisch centrum aanbiedt. Met deze app wil zij toegang tot locatiedata (GPS), zodat de bezoekers op de kaart kunnen zien waar zij zich op de route bevinden.

Een gebruiker zal **voordat** de app informatie van het apparaat haalt of daar informatie op plaatst **geïnformeerd** moeten worden dat de app gebruik maakt van GPS met als **doel** de interactieve route te laten functioneren zodat het cultureel erfgoed van Amsterdam op de digitale kaart bekeken kan worden. Een mogelijke manier van informeren zou zijn door de doelomschrijving op te nemen in een schermmelding in de interface van de app **voordat**

toestemming wordt gegeven (ingevolge het CBP). Wanneer dit wordt gegeven zal de app toegang krijgen tot de GPS van de gebruiker.

Let op! Als een gebruiker geen toestemming geeft voor de verwerking van een bepaald persoonsgegeven kan een praktisch gevolg zijn dat de app niet goed- en/of helemaal niet werkt. Denk hierbij bijvoorbeeld aan de functionaliteit van GPS, als een app dit nodig heeft om bepaalde locaties te tonen.

3.3 Toestemming intrekken

De Artikel 29-werkgroep geeft aan dat een gebruiker van een app altijd de mogelijkheid moet hebben de toestemming van een bepaalde verwerking van een persoonsgegeven weer in te trekken. De Artikel 29-werkgroep geeft daarnaast ook nog aan dat de gebruiker de app moet kunnen de-installeren en de verzamelde persoonsgegevens moet kunnen verwijderen. Via een Apple of Android smartphone is er bijvoorbeeld de mogelijkheid om GPS weer uit te zetten of een bepaalde app te verwijderen.

4. Pushberichten versturen binnen een app

Om vast te kunnen stellen wat juridisch wel en niet mag bij het verzenden van pushberichten, moet ook gekeken worden naar de e-mailregelgeving die is opgenomen in de Telecommunicatiewet. De toezichthouder van de Telecommunicatiewet is de Autoriteit Consument en Markt (ACM).

4.1 Toestemming pushbericht

Volgens de Telecommunicatiewet heeft u, voor u commerciële, charitatieve of ideële e-mail verstuurt, voorafgaande toestemming nodig van de ontvanger van de e-mail (opt-in). Dit geldt ook voor pushberichten. Bij een app dient u toestemming te vragen om commerciële, charitatieve of ideële pushberichten te mogen versturen. De volgende zaken zijn hierbij belangrijk:

- De ontvanger dient zijn toestemming te geven. Dit kan bijvoorbeeld door middel van het digitaal aanvinken van een hokje in de app (deze mag niet vooraf zijn aangevinkt) of door akkoord te geven op een pop-up in de app. Dit dient te gebeuren vóór het verzenden van het eerste pushbericht.
- Bij de toestemmingsvraag moet in een bij- of onderschrift vermeld worden dat de app pushberichten zendt. Dit moet voor de ontvanger direct duidelijk zijn. U mag niet alleen verwijzen naar uw algemene voorwaarden of privacy statement, dit is onvoldoende.

4.2 Afmelden pushberichten

Gebruikers moeten altijd de mogelijkheid hebben zich weer af te melden voor de pushberichten. Dit staat bekend als het Recht van verzet. Dit kan op app-niveau en/of op telefoonniveau.

Apple biedt in de iOS 3 en 4 de mogelijkheid om alle pushberichten in een keer uit te schakelen. Dit kan door: Instellingen/Berichtgeving/Schakelaar op uitzetten. In de iOS 5/6/7 is de schakelaar weggehaald en vervangen door het Berichtencentrum (onder Instellingen). Hierin kunt u de pushberichten per app aan-/uitzetten.

Bij Android toestellen dient voor afmelden van pushberichten in de instellingen van de betreffende app zelf gekeken te worden.

Praktijkvoorbeeld toestemming & toestemming intrekken

Kledingwinkel *het Jasje* heeft een app ontwikkeld waarin de collectie van de winkel uitgebreid bekeken kan worden. Wanneer deze collectie wordt aangevuld met nieuwe kledingstukken stuurt de app een pushbericht naar de gebruiker. Voordat kledingwinkel *het Jasje* dit mag doen is toestemming van de gebruiker nodig. Ook dient het voor de gebruiker duidelijk te zijn dat de app pushberichten verzendt.

In de app van kledingwinkel *het Jasje* is in de instellingen een mogelijkheid opgenomen waar gebruikers zich weer kunnen afmelden voor de pushberichten. Dit is gedaan op de volgende manier in de instellingen van de app:

☐ *Ik wil geen pushberichten meer ontvangen van kledingwinkel het Jasje.*

5. Vermelden bedrijfsgegevens in app

Ook het Burgerlijk Wetboek (BW) biedt een juridisch kader voor mobile. Namelijk artikel 3:15d BW. Dit artikel regelt dat een organisatie die een dienst van de informatiemaatschappij aanbiedt, zijn gegevens moet tonen. Het gaat hierbij in ieder geval om de volgende gegevens die in de app opgenomen moeten worden:

- Naam
- Woonplaats
- E-mailadres
- KVK-nummer

Wanneer er bij een app vergunningen horen, of de app bepaalde zaken van een beroepsgroep regelt (bijv. advocaten of artsen) moet dit ook vermeld worden.

6. Cookies

In dit document mogen ook de regels over cookies niet ontbreken. Zowel apps als mobile sites kunnen cookies plaatsen. Als een app of mobile site cookies plaatst moeten de gebruikers hierover duidelijk en volledig geïnformeerd worden en dient er toestemming gegeven te worden. De wettelijke toezichthouder op het naleven van de Telecommunicatiewet, de ACM, zegt het volgende over informeren en toestemming.

6.1 Informeren over cookies

Informeren kan niet door een vage verwijzing naar een privacy statement. Een privacy statement is wel geschikt om nadere uitleg te verstrekken en bijvoorbeeld de werking van de cookies die uw website plaatst te benoemen. In uw privacy statement moet u dan de volgende zaken vermelden:

- Welke cookies worden geplaatst
- Voor welk doel (bezoekersaantallen registreren, plaatjes laden, Online Behavioral Advertising)
- Welke informatie met een cookie wordt vastgelegd
- Of de informatie verstrekt wordt aan derden

De informatie over het plaatsen van cookies moet op een zichtbare plek staan, met een begrijpelijke uitleg waarom u het cookie plaatst en welke informatie met welk doel wordt verzameld.

6.2 Toestemming voor het plaatsen cookies

De tweede verplichting is dat u toestemming moet vragen voor het plaatsen van cookies. De toestemming geldt niet voor cookies die noodzakelijk zijn. Voorbeelden van noodzakelijke cookies zijn:

- Cookies die gebruikt worden bij het onthouden van items in een winkelmandje
- Cookies om inloggegevens te onthouden

U kan op dit moment op meerdere manieren toestemming voor het plaatsen van de cookies vragen. Dit kan bijvoorbeeld via een pop-up of een banner waarmee u toestemming kunt

vragen voor het plaatsen van cookies. De regering denkt intussen ook na over een model van impliciete toestemming en een uitzondering voor 'analytics cookies'.

6.2.1 Uitzondering: toestemming analytics cookies

Op verzoek van de Tweede Kamer heeft Minister Kamp in mei 2013 een voorstel tot een wetswijziging opgesteld. Hier worden bij cookies die weinig impact hebben op de privacy van de bezoeker uitgezonderd van de verplichting om toestemming te vragen. Denk hierbij aan analytics cookies die op geaggregeerd niveau websitebezoeken meten.

6.2.2 Geïnformeerde consent

De Tweede Kamer vindt zogenaamde cookiemuren niet gebruiksvriendelijk. Dit zijn de modellen waarbij de webbezoeker wordt gedwongen een keuze te maken in het accepteren van cookies, voor hij kan doorsurfen op een website. Sommige websites weigeren bezoekers als zij geen cookies accepteren. Daarom kijkt de regering nu of er op een gebruiksvriendelijkere manier toestemming gevraagd kan worden. Dit betekent waarschijnlijk dat een bezoeker niet expliciet hoeft aan te geven of hij wel of geen cookies wil. Als een website hem eerst duidelijk en volledig informeert over het plaatsen van de cookies, een keuze biedt, en de bezoeker vervolgens doorsurft, wordt dit ook geacht toestemming te zijn (geïnformeerde consent).

6.3 Privacy en cookies

In Europa is veel discussie gaande of een cookie wel of geen persoonsgegeven is. Een cookie herkent immers een pc of telefoon, maar niet een individu. Indien er sprake is van cookies die gebruikers over tijd en over meerdere websites volgen ('tracking cookies') geldt de

privacywetgeving. Dit zou dan betekenen dat ook de regels uit de Wbp van toepassing zijn op cookies (naast de regels uit de Telecommunicatiewet). Zorg dus dat u in het vizier hebt of u cookies gebruikt voor het monitoren van surfgedrag. Kijk voor meer informatie over cookies in het juridisch loket van DDMA: http://ddma.nl/juridisch-loket/dossiers/cookies/

7. Overige mobile diensten

In deze paragraaf worden nog de SMS/MMS- en Bluetooth functie besproken.

7.1 SMS/MMS

Een SMS sturen naar een 06-nummer kan vergeleken worden met het toesturen van een e-mail. Voor het versturen van een SMS geldt (op basis art. 11.7 Telecommunicatiewet) een opt-in regime. Er is dus toestemming van de consument nodig om hem per SMS te mogen benaderen.

7.2 Bluetooth

De reclameactiviteit via Bluetooth valt vooralsnog niet onder de Telecommunicatiewet. Bij Bluetooth worden berichten onafhankelijk van een bepaald openbaar elektronisch communicatienetwerk en onafhankelijk van een elektronisch communicatiedienst verstuurd. De Telecommunicatiewet is hierop niet van toepassing, omdat er geen sprake is van een openbare elektronische communicatiedienst. Op de smartphone of tablet kan worden ingesteld dat een toestel niet zichtbaar is voor deze reclame (Recht van verzet). Wel kan Bluetooth onder de Wbp vallen. Dit als Bluetooth zichtbaar is op bijvoorbeeld een smartphone. Bij het verwerken van Bluetooth verkeer kan het unieke MAC-adres van het toestel worden verzameld en verwerkt. Wanneer dit gebeurd in combinatie met locatiegegevens van het toestel is er sprake van een verwerking van persoonsgegevens waarop de Wbp van toepassing is.

8. Toezicht op mobile & achtergrondinformatie

In deze paragraaf wordt kort ingegaan op het toezicht op de wetgeving met betrekking tot mobile.

8.1 Wie houdt toezicht op mobile in Nederland?

CBP en ACM houden toezicht op de naleving van de wet- en regelgeving voor mobile. Zij controleren of bedrijven/organisaties zich aan de regelgeving met betrekking tot mobile houden en kunnen hierbij handhaven.

8.2 Achtergrondinformatie

- DDMA juridisch loket over persoonsgegevens: http://ddma.nl/juridisch-loket/dossiers/wet-bescherming-persoonsgegevens/
- DDMA juridisch loket over cookies: http://ddma.nl/juridisch-loket/dossiers/cookies/
- Opinie CBP: http://www.cbpweb.nl/Pages/pb_20130314-wp29-opinie-mobiele-apps.aspx
- CBP: 'Mijn privacy' over apps: http://www.mijnprivacy.nl/Vraag/Apps/Paginas/Apps.aspx

Mocht u als lid vragen hebben over wat wel en niet mag bij mobile dan kunt telefonisch of per e-mail contact opnemen met de juristen op het DDMA bureau: info@ddma.nl of 020-4528413.

Over DDMA

DDMA is de branchevereniging voor dialoogmarketing. DDMA biedt deskundige en praktische kennis over datadrivenmarketing, waarbij relevantie van reclame en respect voor privacy centraal staan. Als service aan onze leden (opdrachtgevers & dienstverleners), als gesprekspartner van Den Haag en Brussel en als promotor van kwaliteit in de sector.

DDMA zet zich in voor de ontwikkeling en kwaliteit van het vakgebied. We doen dit al jaren in onze commissies, bijeenkomsten en via branche-onderzoeken. DDMA formuleert kwaliteitseisen voor het vakgebied, en leden committeren zich aan de afspraken over integere commerciële communicatie. DDMA controleert organisaties op het gebruik van data voor marketing. Gebruiken de leden die data goed, dan mogen zij het Privacy Waarborg voeren. Het Privacy Waarborg is een keurmerk waarmee organisaties hun relaties (B2B en B2C) laten zien dat zij op een correcte manier contactgegevens gebruiken voor reclamedoeleinden.

Indien u vragen heeft met betrekking tot mobile, kunt u altijd terecht bij het online juridisch loket. Het juridisch loket van DDMA is te bereiken via: www.ddma.nl/juridisch-loket Telefonisch advies over wat juridisch wel en niet mag is voorbehouden aan DDMA-leden. Lid worden? Kijk op www.ddma.nl/lidmaatschap of neem contact op met het DDMA-bureau:

DDMA-bureau
W.G. Plein 507/508
1054 SJ Amsterdam

Telefoonnummer: 020-4528413
E-mail: info@ddma.nl

Disclaimer

Deze juridische tips mobile (verder te noemen: “Tips Mobile”) van DDMA zijn met grote zorg en precisie samengesteld. Ondanks de inspanning en aandacht voor deze Tips Mobile van DDMA is het mogelijk dat informatie onvolledig, niet langer juist of onjuist is. DDMA sluit hierbij alle aansprakelijkheid uit voor schade, van welke aard dan ook, die voortvloeit uit of verband houdt met het gebruik van deze Tips Mobile van DDMA.

DDMA september 2013

Bijlage: Checklist mobile

De artikel 29 werkgroep (samenwerkingsverband alle privacytoezichthouders EU) heeft regelgeving uit de Wet bescherming persoonsgegevens (Wbp) vertaald naar het gebruik van apps. In deze checklist worden de belangrijkste voorwaarden besproken met betrekking tot de verwerking van persoonsgegevens door apps. Aan de hand van deze checklist kunt u nagaan of uw app voldoet aan deze regels van het CBP. De belangrijkste voorwaarden worden in de checklist besproken. Daarnaast wordt er ingegaan op het verzenden van pushberichten, cookies, SMS en Bluetooth binnen mobile. Zie voor een uitgebreide uitleg ook het document praktische juridische tips mobile.

1. Moet de app-gebruiker toestemming geven voordat de app informatie plaatst of uitleest van zijn randapparatuur? (zie paragraaf 2.2 document)
Omdat een app per definitie informatie plaatst op of leest van randapparatuur valt hij daarmee onder het toestemmingsvereiste van de cookiewet en de e-privacy richtlijn.

2. Verwerkt u persoonsgegevens binnen een app? (zie paragraaf 1.1 document)
Indien nee ga dan naar vraag 7.
Een persoonsgegeven is een gegeven dat direct of indirect herleidbaar is tot een individu. Dit zijn bijvoorbeeld contacten, locatie-informatie, creditcardinformatie, foto's en video's en login-gegevens van social media. Sommige apps maken gebruik van deze gegevens.

3. Informeert u de app-gebruiker over het gebruik van persoonsgegevens en met welk doel, voordat de app informatie van het apparaat haalt of daar op plaatst? (zie paragraaf 3.1 document)
U moet duidelijke en begrijpbare doelen aangeven van de verwerking van de persoonsgegevens. Deze doelen mogen niet zomaar tussentijds gewijzigd worden. De essentiële informatie met betrekking tot de verwerking van deze doelen dient, voordat de gebruiker van de app toestemming geeft, zichtbaar te worden

gemaakt. Dit kan bijvoorbeeld vanuit de downloadomgeving. Het CBP geeft in correspondentie echter aan dat de app-bouwer in zijn interface zelf zal moeten voorzien in specifieke informatie welke gegevens door hem voor welke doel worden verwerkt en hoelang de gegevens door hem worden bewaard.

4. Vraagt u apart toestemming voor de categorieën gegevens waar de app toegang tot heeft? (zie paragraaf 3.2 document)

De Artikel 29-werkgroep geeft in haar opinie aan dat er apart toestemming moet worden gevraagd voor het verwerken van de categorieën gegevens waar de app toegang tot heeft. Dit is bijvoorbeeld toestemming voor toegang tot GPS of toegang tot een contactenlijst.

5. Heeft de gebruiker van de app de mogelijkheid de toestemming in te trekken?(zie paragraaf 3.3 document)

Een gebruiker van een app moet altijd de mogelijkheid hebben de toestemming van een bepaalde verwerking van een persoonsgegeven weer in te trekken. Via een Apple of Android smartphone is er bijvoorbeeld de mogelijkheid om GPS weer uit te zetten.

6. Zijn er voldoende technische maatregelen genomen waardoor de persoonlijke gegevens die gebruikt worden door de app beveiligd zijn? (zie paragraaf 2.5 document)

U moet technische maatregelen nemen zodat de persoonlijke gegevens die gebruikt worden door de app, goed beveiligd zijn. De Artikel 29-werkgroep geeft als aanbeveling dat u gebruikers actief dient te informeren als er een datalek heeft plaatsgevonden.

7. Vraagt u de gebruiker van uw app voorafgaande toestemming bij het verzenden van pushberichten en informeert u de gebruiker hierover? (zie paragraaf 4.1 document)

Bij een app dient u toestemming te vragen om commerciële, charitatieve of ideële pushberichten te mogen versturen. Dit kan bijvoorbeeld doormiddel van het digitaal aanvinken van een hokje (deze mag niet vooraf zijn aangevinkt). Dit dient te gebeuren vóór het verzenden van het eerste pushbericht. Bij de

toestemmingsvraag moet in een bij- of onderschrift duidelijk gemaakt worden dat de app gebruikt zal worden voor bijvoorbeeld het toezenden van pushberichten.

8. Heeft de gebruiker de mogelijkheid zich af te melden voor de pushberichten? (zie paragraaf 4.2 document)

Gebruikers moeten altijd de mogelijkheid hebben zich weer af te melden voor de pushberichten. Dit kan op app-niveau en/of op telefoonniveau.

9. Noemt u ergens in uw app uw bedrijfsgegevens? (zie paragraaf 5 document)

Het gaat hier in ieder geval om uw bedrijfsnaam, woonplaats, e-mail en KvK nummer.

10. Wanneer u een app ontwikkelt voor kinderen, denkt u dan aan de voorwaarden hiervoor? (zie paragraaf 2.6 document)

Wanneer er persoonsgegevens worden verwerkt van een minderjarig kind (jonger dan 16 jaar) moeten de ouders hiervoor toestemming geven. Ook is het niet toegestaan om gegevens van kinderen onder de 13 jaar te gebruiken om selecties te maken voor advertenties gericht op deze groep.

11. Maakt u gebruik van cookies/SMS/Bluetooth binnen mobile? Zie hiervoor het document praktische juridische tips mobile. (zie paragraaf 6 en 7 document)