GROEP GEGEVENSBESCHERMING ARTIKEL 29

00461/13/NL
WP 202

Advies 02/2013 over apps op intelligente apparaten

Goedgekeurd op 27 februari 2013

Samenvatting

Applicatiewinkels bieden honderdduizenden verschillende applicaties (“apps”) aan voor alle populaire soorten intelligente apparaten. Naar verluidt worden er dagelijks meer dan 1 600 nieuwe apps door applicatiewinkels aangeboden. Volgens onderzoeken downloadt de gemiddelde smartphonegebruiker 37 apps. Apps worden niet zelden gratis of tegen een lage aanschafprijs aangeboden aan eindgebruikers; de gebruikersgroep kan uiteenlopen van een paar personen tot vele miljoenen gebruikers.

Apps zijn in staat grote hoeveelheden gegevens uit het apparaat te verzamelen (bijv. gegevens die op het apparaat zijn opgeslagen door de gebruiker en gegevens afkomstig van verschillende sensoren, inclusief de locatie) en deze te verwerken om de eindgebruiker nieuwe en innovatieve diensten te verlenen. Diezelfde gegevensbronnen kunnen echter aan verdere verwerking worden onderworpen, doorgaans om opbrengsten te genereren, op manieren die voor de eindgebruiker onbekend of ongewenst zijn.

App-ontwikkelaars die zich niet bewust zijn van de vereisten voor gegevensbescherming kunnen aanzienlijke risico’s creëren voor de persoonlijke levenssfeer en de reputatie van de gebruikers van intelligente apparaten. De belangrijkste risico’s voor eindgebruikers op het gebied van gegevensbescherming zijn het gebrek aan transparantie en kennis met betrekking tot de verwerking door apps, gecombineerd met het ontbreken van geldige toestemming voordat verwerking plaatsvindt. Slechte beveiligingsmaatregelen, een duidelijke trend in de richting van maximale gegevensinzameling en de rekbaarheid van de doelen waarvoor persoonsgegevens worden verzameld, dragen verder bij aan de risico’s die de huidige markt voor apps met zich meebrengt op het gebied van gegevensbescherming.

Een groot gevaar voor de gegevensbescherming wordt bovendien gevormd door de mate van fragmentatie als gevolg van het grote aantal spelers op het gebied van app-ontwikkeling. Hiertoe behoren: app-ontwikkelaars, app-eigenaars, app-winkels, fabrikanten van besturingssystemen en apparaten, alsmede overige derden die betrokken zijn bij de verzameling en verwerking van persoonsgegevens uit intelligente apparaten, zoals aanbieders van onderzoeks- en reclamediensten. Het merendeel van de conclusies en aanbevelingen in dit advies is bestemd voor de ontwikkelaars van apps (aangezien zij de meeste invloed hebben op de exacte wijze waarop de verwerking plaatsvindt of informatie in de app wordt weergegeven). Om te kunnen voldoen aan de strengste normen voor privacy- en gegevensbescherming moeten zij echter dikwijls samenwerken met andere partijen uit de app-sector. Dit is van bijzonder belang voor de beveiliging, die wordt gegarandeerd door een keten van meerdere partijen, die zo sterk is als de zwakste schakel.

Veel van de gegevens die zich op een intelligent mobiel apparaat bevinden, zijn persoonsgegevens. Het toepasselijke wettelijke kader wordt in dit geval gevormd door de richtlijn gegevensbescherming, gecombineerd met de bescherming van mobiele apparaten voor zover deze deel uitmaken van de privésfeer van gebruikers zoals voorzien in de e-privacyrichtlijn. Deze regels zijn van toepassing op iedere app bestemd voor app-gebruikers in de Unie, ongeacht de locatie van de app-ontwikkelaar of de app-winkel.

In dit advies geeft de werkgroep een toelichting op het wettelijk kader dat van toepassing is op de verwerking van persoonsgegevens bij de ontwikkeling, distributie en gebruik van apps op intelligente apparaten, waarbij de nadruk wordt gelegd op het toestemmingsvereiste, de beginselen van doelbinding en minimale gegevensinzameling, de noodzaak om gepaste beveiligingsmaatregelen te nemen, de plicht om eindgebruikers op correcte wijze te informeren, hun rechten, redelijke bewaartermijnen en in het bijzonder de eerlijke verwerking van gegevens die verkregen zijn van en over kinderen.

Inhoud

1. Inleiding

Apps zijn softwaretoepassingen die vaak ontworpen zijn voor specifieke taken en die bestemd zijn voor een bepaald soort intelligente apparaten, zoals smartphones, tablets en televisietoestellen met internetverbinding. Zij ordenen informatie op een wijze die past bij de specifieke kenmerken van het apparaat en werken nauw samen met de functies van de hardware en het besturingssysteem die op het apparaat aanwezig zijn.

Applicatiewinkels bieden honderdduizenden verschillende apps aan voor alle populaire soorten intelligente apparaten. Apps kennen een grote verscheidenheid aan gebruiksmogelijkheden, waaronder browsen op internet, communicatie (e-mail, telefonie en berichtenuitwisseling via internet), amusement (games, films/video's en muziek), sociale netwerken, internetbankieren en locatiegebaseerde diensten. Naar verluidt worden er dagelijks meer dan 1 600 nieuwe apps door applicatiewinkels aangeboden[1]. Volgens onderzoeken downloadt de gemiddelde smartphonegebruiker 37 apps[2]. Apps worden niet zelden gratis of tegen een lage aanschafprijs aangeboden aan eindgebruikers; de gebruikersgroep kan uiteenlopen van een paar personen tot vele miljoenen gebruikers.

Het onderliggende besturingssysteem bevat bovendien software of gegevensstructuren die van belang zijn voor de kerndiensten die het intelligente apparaat biedt, bijvoorbeeld het adresboek van een smartphone. Het besturingssysteem is ontworpen om deze componenten beschikbaar te stellen aan apps door middel van "application programming interfaces" (API's). Dergelijke API's bieden toegang tot een veelvoud aan sensoren die op intelligente apparaten aanwezig kunnen zijn. Voorbeelden van dergelijke sensoren zijn: een gyroscoop, een digitaal kompas en een versnellingsmeter die informatie over de aangehouden snelheid en richting biedt, camera's aan voor- en achterzijde om video's en foto's te maken, en een microfoon om geluid op te nemen. Intelligente apparaten kunnen ook afstandssensoren bevatten[3]. Intelligente apparaten kunnen ook verbindingen tot stand brengen door middel van een groot aantal netwerkinterfaces, zoals Wi-Fi, Bluetooth, NFC of Ethernet. Tot slot kunnen locaties nauwkeurig worden bepaald door middel van geolocatiediensten (zoals beschreven in het advies van de Groep artikel 29 over geolocatiediensten op slimme mobiele apparaten[4]). De soort, nauwkeurigheid en frequentie van deze sensorgegevens verschilt per apparaat en besturingssysteem.

Dankzij API's kunnen app-ontwikkelaars voortdurend dit soort gegevens verzamelen, toegang krijgen tot contactgegevens en deze vastleggen, e-mails, sms-berichten en berichten op sociale netwerken versturen, de inhoud van SD-kaarten lezen/wijzigen/wissen, geluid opnemen, de camera gebruiken en toegang krijgen tot opgeslagen foto's, de status en de identiteit van de telefoon bekijken, de algemene systeeminstellingen wijzigen en voorkomen dat de telefoon de slaapstand activeert. API's kunnen ook informatie verschaffen over het apparaat zelf aan de hand van een of meer unieke identificatiecodes en informatie over andere apps die op het apparaat geïnstalleerd zijn. Deze gegevensbronnen kunnen aan

---

1 Rapportage in ConceivablyTech van 19 augustus 2012, beschikbaar op: http://www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of.
Geciteerd door Kamala D. Harris, procureur-generaal van het California Department of Justice, in: "Privacy on the Go: Recommendations for the Mobile Ecosystem", januari 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

2 Dit is een wereldwijde schatting voor 2012 van ABI Research (http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o).

3 Dit is een sensor die de aanwezigheid van een voorwerp kan waarnemen zonder fysiek contact. Zie: http://www.w3.org/TR/2012/WD-proximity-20121206/.

4 Zie Advies 13/2011 van de Groep Artikel 29 over geolocatiediensten op slimme mobiele apparaten (mei 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_nl.pdf.

verdere verwerking worden onderworpen, doorgaans om opbrengsten te genereren, op manieren die voor de eindgebruiker onbekend of ongewenst zijn.

Het doel van dit advies is een toelichting te geven op het wettelijk kader dat van toepassing is op de verwerking van persoonsgegevens bij de distributie en het gebruik van apps op intelligente apparaten en te beoordelen aan wat voor verwerkingen de gegevens buiten de app kunnen worden onderworpen, zoals het gebruik van de verzamelde gegevens om profielen samen te stellen en gebruikers te benaderen. In dit advies worden de belangrijkste risico's op het gebied van gegevensbescherming geanalyseerd, wordt een beschrijving geboden van de diverse betrokken partijen en wordt een toelichting gegeven op de diverse wettelijke verplichtingen. Tot deze partijen behoren: app-ontwikkelaars, app-eigenaars en app-winkels, fabrikanten van besturingssystemen en apparaten, en overige derden die betrokken zijn bij de verzameling en verwerking van persoonsgegevens uit intelligente apparaten, zoals aanbieders van onderzoeks- en reclamediensten.

Het advies besteedt vooral aandacht aan het toestemmingsvereiste, de beginselen van doelbinding en minimale gegevensinzameling, de noodzaak om gepaste beveiligingsmaatregelen te nemen, de plicht om eindgebruikers op correcte wijze te informeren, hun rechten, redelijke bewaartermijnen en in het bijzonder de redelijke verwerking van gegevens die verkregen zijn van en over kinderen.

Het advies kan worden toegepast op vele verschillende soorten intelligente apparaten, maar is vooral gericht op apps bestemd voor intelligente mobiele apparaten.

2. Risico's op het gebied van gegevensbescherming

Door de nauwe interactie met het besturingssysteem kunnen apps tot aanzienlijk meer gegevens toegang krijgen dan traditionele webbrowsers[5].
Apps zijn in staat grote hoeveelheden gegevens uit het apparaat te verzamelen (locatiegegevens, gegevens die op het apparaat zijn opgeslagen door de gebruiker en gegevens afkomstig van de verschillende sensoren) en deze te verwerken om de eindgebruiker nieuwe en innovatieve diensten te verlenen.

Een groot gevaar voor de gegevensbescherming wordt gevormd door de mate van fragmentatie als gevolg van het grote aantal spelers op het gebied van app-ontwikkeling. Een enkel gegevensonderdeel kan direct vanaf het apparaat verzonden worden om wereldwijd te worden verwerkt of te worden gekopieerd door ketens van derden. Sommige van de meest bekende apps zijn ontwikkeld door grote technologiebedrijven, maar veel andere apps worden ontworpen door kleine startende ondernemingen. Een enkele programmeur met een idee en weinig tot geen eerdere programmeerervaring kan binnen korte tijd een wereldwijd publiek bereiken. App-ontwikkelaars die zich niet bewust zijn van de vereisten voor gegevensbescherming kunnen aanzienlijke risico's creëren voor de persoonlijke levenssfeer en de reputatie van de gebruikers van intelligente apparaten. Daarbij komt dat de diensten van derden, zoals reclamediensten, een snelle ontwikkeling doormaken. Als een app-ontwikkelaar deze zonder de gepaste zorg te betrachten in de applicatie integreert, kunnen daardoor aanzienlijke hoeveelheden persoonsgegevens bekend worden gemaakt.

De belangrijkste risico's voor eindgebruikers op het gebied van gegevensbescherming zijn het gebrek aan transparantie en kennis met betrekking tot de verwerking door apps, gecombineerd met het ontbreken van geldige toestemming voordat verwerking plaatsvindt. Slechte beveiligingsmaatregelen, een duidelijke trend in de richting van maximale gegevensinzameling en de rekbaarheid van de doelen

[5] Hoewel webbrowsers op desktops ook steeds meer toegang krijgen tot sensorgegevens uit de apparaten van eindgebruikers, gestimuleerd door de ontwikkelaars van webgames.

waarvoor persoonsgegevens worden verzameld, dragen verder bij aan de risico's die de huidige markt voor apps met zich meebrengt op het gebied van gegevensbescherming. Veel van deze risico's zijn al eerder onderzocht en geregeld door andere internationale toezichthouders, zoals de Amerikaanse Federal Trade Commission, het Canadese Bureau voor privacybescherming en de procureur-generaal van het California Department of Justice[6].

- Een van de voornaamste risico's op het gebied van gegevensbescherming is het gebrek aan transparantie. App-ontwikkelaars worden beperkt door de mogelijkheden die worden geboden door de fabrikanten van besturingssystemen en door app-winkels wanneer zij ervoor willen zorgen dat op het juiste moment volledige informatie aan de eindgebruiker wordt geboden. Veel app-ontwikkelaars maken echter geen gebruik van deze mogelijkheden. Veel apps beschikken namelijk niet over privacynormen of verzuimen hun potentiële gebruikers op begrijpelijke wijze te informeren over het soort persoonsgegevens dat de app kan verwerken en de doeleinden waarvoor dit gebeurt. Het gebrek aan transparantie beperkt zich niet tot gratis apps of apps van onervaren ontwikkelaars: een recent onderzoek laat zien dat slechts 61,3 % van de 150 meest gebruikte apps over een privacybeleid beschikt[7].

- Het gebrek aan transparantie is nauw gerelateerd aan het ontbreken van vrije en geïnformeerde toestemming. Na het downloaden van de app blijft de toestemming vaak beperkt tot een hokje dat aangevinkt moet worden ten teken dat de eindgebruiker akkoord gaat met de gebruiksvoorwaarden, zonder zelfs maar de optie "Nee, bedankt" aan te bieden. Volgens een onderzoek van GSMA uit september 2011 wil 92 % van de app-gebruikers een meer gespecificeerde keuze krijgen[8].

- Ontoereikende beveiligingsmaatregelen kunnen leiden tot ongeautoriseerde verwerking van (gevoelige) persoonsgegevens, bijvoorbeeld wanneer er bij een app-ontwikkelaar een inbreuk op persoonsgegevens plaatsvindt of de app zelf persoonsgegevens lekt.

- Een ander risico voor de gegevensbescherming houdt verband met de veronachtzaming (door onwetendheid of met opzet) van het beginsel van doelbinding, op grond waarvan persoonsgegevens alleen mogen worden verzameld en verwerkt voor specifieke en legitieme doeleinden. Persoonsgegevens die door apps worden verzameld, kunnen op grote schaal worden verspreid onder derden ten behoeve van vage of rekbare doeleinden als "marktonderzoek". Dezelfde verontrustende veronachtzaming doet zich voor ten aanzien van het beginsel van gegevensminimalisering. Recent onderzoek laat zien dat veel apps grote hoeveelheden gegevens uit smartphones verzamelen zonder dat er een redelijk verband bestaat met de kennelijke functionaliteit van de app[9].

---

6 Zie onder andere het FTC-rapport "Mobile Privacy Disclosures: Building Trust Through Transparency", februari 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; het FTC-rapport "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing", februari 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; en het vervolgrapport "Mobile Apps for Kids: Disclosures Still Not Making the Grade", december 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; het rapport van het Canadese Bureau voor privacybescherming "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps", oktober 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf; Kamala D. Harris, procureur-generaal van het California Department of Justice: "Privacy on the Go: Recommendations for the Mobile Ecosystem", januari 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

7 FPF-onderzoek uit juni 2012 over mobiele apps, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

8 "89 % [van de gebruikers] vindt het belangrijk om te weten wanneer hun persoonsgegevens door een app worden gedeeld, alsook om dit uit of aan te kunnen zetten." Bron: "User perspectives on mobile privacy", september 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

9 Wall Street Journal, "Your Apps Are Watching You", http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

3 Beginselen inzake gegevensbescherming

3.1 Toepasselijk recht

Het toepasselijk wettelijk kader wordt gevormd door de richtlijn gegevensbescherming (95/46/EG). Deze is van toepassing in iedere situatie waarbij het gebruik van apps op intelligente apparaten de verwerking van persoonsgegevens met zich meebrengt. Om vast te stellen welke normen van toepassing zijn, is het essentieel om eerst vast te stellen wat de rol is van de diverse betrokkenen: met name de vaststelling van de verantwoordelijke voor de verwerking via de mobiele apps is van doorslaggevend belang voor het toepasselijk recht. Waar de voor de verwerking verantwoordelijke is gevestigd, is bepalend voor de toepassing van de EU-wetgeving betreffende gegevensbescherming. Volgens artikel 4, lid 1, onder a), van de richtlijn gegevensbescherming is het nationale recht van een lidstaat van toepassing op de verwerking van persoonsgegevens die plaatsvindt "in het kader van de activiteiten van een vestiging" van de voor de verwerking verantwoordelijke op het grondgebied van de betreffende lidstaat. Volgens artikel 4, lid 1, onder c), van de richtlijn gegevensbescherming is het nationale recht van een lidstaat ook van toepassing indien de voor de verwerking verantwoordelijke *niet gevestigd* is op het grondgebied van de Gemeenschap, maar voor de verwerking van persoonsgegevens wel gebruikmaakt van middelen die zich op het grondgebied van genoemde lidstaat bevinden. Aangezien het gebruikte apparaat nodig is bij de verwerking van persoonsgegevens van en over de gebruiker, wordt doorgaans aan deze voorwaarde voldaan[10]. Dit is echter alleen relevant wanneer de voor de verwerking verantwoordelijke niet in de Unie gevestigd is.

Bijgevolg, wanneer een partij die betrokken is bij de ontwikkeling, distributie en exploitatie van apps geacht wordt verantwoordelijk voor de verwerking te zijn, dan is deze partij – persoonlijk of samen met anderen – aansprakelijk voor de naleving van alle voorschriften van de richtlijn gegevensbescherming. De vaststelling van de rol van de bij mobiele apps betrokken partijen zal onder punt 3.3 verder worden geanalyseerd.

Naast de richtlijn gegevensbescherming schrijft de e-privacyrichtlijn (2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG) specifieke normen voor aan alle partijen wereldwijd die informatie die opgeslagen is op de apparaten van gebruikers in de Europese Economische Ruimte (EER) willen opslaan of daartoe toegang willen hebben.

Artikel 5, lid 3, van de e-privacyrichtlijn bepaalt dat *de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. (...)*

Hoewel veel bepalingen van de e-privacyrichtlijn alleen van toepassing zijn op aanbieders van openbare elektronischecommunicatienetwerken of -diensten in de Gemeenschap, is artikel 5, lid 3, van toepassing op iedere entiteit die informatie op intelligente apparaten plaatst of inziet. Dit artikel geldt ongeacht de aard van de entiteit (d.w.z. ongeacht of het een publieke of private entiteit betreft, een individuele programmeur of een grote onderneming, de voor de verwerking verantwoordelijke, de verwerker of een derde).

[10] Voor zover de app verkeer van persoonsgegevens met voor de verwerking verantwoordelijke partijen oplevert. Aan dit criterium wordt mogelijk niet voldaan als de gegevens uitsluitend ter plaatse, in het apparaat zelf, worden verwerkt.

Het toestemmingsvereiste van artikel 5, lid 3, geldt voor alle informatie, ongeacht de aard van de opgeslagen of geraadpleegde informatie. De werkingssfeer is niet beperkt tot persoonsgegevens; het betreft iedere soort informatie die op het apparaat is opgeslagen.

Het toestemmingsvereiste van artikel 5, lid 3, van de e-privacyrichtlijn geldt voor diensten die '*in de Gemeenschap*' worden aangeboden, dat wil zeggen, aan alle personen die in de Europese Economische Ruimte wonen, ongeacht de locatie van de dienstverlener. Het is voor app-ontwikkelaars belangrijk om te weten dat beide richtlijnen dwingend recht zijn, in de zin dat de rechten van de betrokken personen onoverdraagbaar zijn en zij hiervan niet bij overeenkomst afstand kunnen doen. Dit betekent dat de toepasselijkheid van de Europese privacywetgeving niet kan worden uitgesloten door een eenzijdige verklaring of contractuele overeenkomst[11].

3.2 Door apps verwerkte persoonsgegevens

Veel van de gegevens die op intelligente apparaten worden opgeslagen of die door deze apparaten worden gegenereerd, zijn persoonsgegevens. Overweging 24 van de e-privacyrichtlijn stelt:

> *"Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist."*

De desbetreffende gegevens worden als persoonsgegevens beschouwd wanneer zij betrekking hebben op een persoon die direct (bijvoorbeeld aan de hand van zijn of haar naam) of indirect kan worden geïdentificeerd door de voor de verwerking verantwoordelijke of een derde. Zij kunnen betrekking hebben op de eigenaar van het apparaat of een andere persoon, zoals contactgegevens van vrienden in een adresboek[12]. De gegevens kunnen op het apparaat worden verzameld en verwerkt, of na verzending via een verbinding met een externe API real-time worden verwerkt, gebruikmakend van de infrastructuur van de app-ontwikkelaar of een derde, zonder dat de eindgebruiker zich hiervan bewust is.

Persoonsgegevens die belangrijke gevolgen kunnen hebben voor het privéleven van gebruikers en andere personen zijn bijvoorbeeld:

- locatie;
- contacten;
- unieke identificatiegegevens van het apparaat en de klant (zoals IMEI[13], IMSI[14], UDID[15] en het mobiele telefoonnummer);
- identiteit van de betrokkene;
- identiteit van de telefoon (d.w.z. de naam van de telefoon[16]);
- creditcard- en betalingsgegevens;
- register van gesprekken, sms-berichten of instant messaging;
- browsergeschiedenis;

---

11 Bijvoorbeeld door een verklaring dat alleen het recht van een land buiten de EER van toepassing is.

12 Gegevens kunnen (i) automatisch worden aangemaakt door het apparaat op basis van eigenschappen die van tevoren zijn vastgesteld door het besturingssysteem en/of de fabrikant van het apparaat of de desbetreffende mobiele-telefoonmaatschappij (bijv. geolocatiegegevens, netwerkinstellingen, IIRSA-Projectenportefeuille-adres); (ii) worden aangemaakt door de gebruiker door middel van apps (contactlijsten, aantekeningen, foto's): (iii) worden aangemaakt door de apps (bijv. browsergeschiedenis).

13 International Mobile Equipment Identity (internationale identiteitsgegevens mobiele apparatuur).

14 International Mobile Subscriber Identity (internationale identiteitsgegevens mobiele abonnee)

15 Unique Device Identifier (unieke identificatiegegevens apparaat).

16 Gebruikers geven doorgaans hun eigen naam aan hun telefoon: "iPhone van Jan Jansen".

- e-mail;
- inloggegevens voor authenticatiediensten op internet (met name diensten die sociaal van aard zijn);
- foto's en video's;
- biometrische informatie (bijv. gezichtsherkenning en vingerafdrukken).

3.3 Bij de gegevensverwerking betrokken partijen

Er zijn veel verschillende partijen betrokken bij de ontwikkeling, distributie en exploitatie van apps; ieder van hen kan verschillende verantwoordelijkheden hebben op het gebied van gegevensbescherming.

Er kunnen vier hoofdgroepen worden onderscheiden: (i) de app-ontwikkelaars (inclusief app-eigenaars)[17], de fabrikanten van besturingssystemen en apparaten ("fabrikanten")[18]; (iii) app-winkels (de distributeur van de app) en ten slotte (iv) overige partijen die betrokken zijn bij de verwerking van persoonsgegevens. In sommige gevallen hebben partijen een gedeelde verantwoordelijkheid, met name wanneer dezelfde entiteit betrokken is bij verschillende fasen, bijvoorbeeld wanneer de fabrikant van een besturingssysteem ook eigenaar is van een app-winkel.
Ook eindgebruikers moeten de verantwoordelijkheid nemen die hun toekomt, aangezien zij persoonsgegevens op hun mobiele apparaten aanmaken en opslaan. Als dit soort verwerking zuiver persoonlijke of huishoudelijke doeleinden dient, is de richtlijn gegevensbescherming niet van toepassing (artikel 3, lid 2) en is de gebruiker vrijgesteld van de formele verplichtingen met betrekking tot gegevensbescherming. Indien gebruikers echter besluiten om hun gegevens door middel van een app te delen, bijvoorbeeld door informatie via een app op een sociaal netwerk bekend te maken aan een onbepaald aantal personen[19] dan verwerken zij informatie die buiten de vrijstelling voor huishoudelijk gebruik valt[20].

3.3.1 App-ontwikkelaars

App-ontwikkelaars maken apps en/of stellen deze beschikbaar aan eindgebruikers. Tot deze categorie behoren ook organisaties uit de private en publieke sector die de ontwikkeling van apps uitbesteden, alsook bedrijven en personen die apps bouwen en implementeren. Zij ontwerpen en/of creëren de software die op smartphones wordt gebruikt en bepalen zo in welke mate de app de verschillende categorieën persoonsgegevens kan raadplegen en verwerken, op het apparaat zelf en/of gebruikmakend van computers op afstand (de computersystemen van de app-ontwikkelaar of derden).
Voor zover de app-ontwikkelaar bepaalt voor welke doeleinden en de wijze waarop persoonsgegevens op intelligente apparaten worden verwerkt, kan hij worden aangemerkt als de voor de verwerking verantwoordelijke zoals bedoeld in artikel 2, onder d), van de richtlijn gegevensbescherming. In dat geval moet hij voldoen aan alle bepalingen van de richtlijn gegevensbescherming. De belangrijkste bepalingen worden uitgelegd in punt 3.4 tot 3.10 van dit advies.

Zelfs wanneer de vrijstelling voor huishoudelijk gebruik van toepassing is op de gebruiker, wordt de app-ontwikkelaar nog steeds aangemerkt als de voor de verwerking verantwoordelijke als hij de gegevens voor zijn eigen doeleinden verwerkt. Dit is bijvoorbeeld het geval wanneer de app toegang

---

[17] De werkgroep hanteert de algemene term "app-ontwikkelaars", maar benadrukt dat de term niet beperkt is tot programmeurs of technische ontwikkelaars van apps, maar ook de eigenaars van apps omvat, dat wil zeggen, bedrijven en organisaties die opdracht geven tot de ontwikkeling van apps en daarvan de doeleinden vaststellen.

[18] In sommige gevallen overlappen de fabrikant van het besturingssysteem en het apparaat elkaar, terwijl in andere gevallen de fabrikant van het apparaat een ander bedrijf is dan de leverancier van het besturingssysteem.

[19] Zie Europees Hof van Justitie, Zaak C-101/01 Strafzaak tegen Bodil Lindqvist, arrest van 6 november 2003 en Zaak C-73/07 Tietosuojavaltuutettu v SatakunnanMarkkinapörssi Oy en Satamedia Oy, arrest van 16 december 2008.

[20] Zie Advies 5/2009 van de Groep artikel 29 over online sociale netwerken (juni 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_nl.pdf.

tot het volledige adresboek nodig heeft om een dienst te kunnen leveren (instant messaging, telefoongesprekken, videogesprekken).

De verantwoordelijkheden van de app-ontwikkelaar zullen aanmerkelijk worden beperkt als er geen persoonsgegevens buiten het apparaat worden verwerkt en/of beschikbaar gesteld, of als de app-ontwikkelaar gepaste technische en organisatorische maatregelen heeft getroffen om ervoor te zorgen dat de gegevens blijvend op het apparaat worden geanonimiseerd en geaggregeerd voordat deze het apparaat verlaten.

Indien de app-ontwikkelaar toegang verkrijgt tot de informatie die op het apparaat is opgeslagen, is de e-privacyrichtlijn in ieder geval ook van toepassing en moet de app-ontwikkelaar voldoen aan het toestemmingsvereiste voorzien in artikel 5, lid 3, van de e-privacyrichtlijn.

Indien de app-ontwikkelaar de feitelijke verwerking geheel of gedeeltelijk uitbesteedt aan een derde partij en deze de rol van verwerker op zich neemt, moet de app-ontwikkelaar voldoen aan alle verplichtingen die betrekking hebben op de inzet van een verwerker. Dit geldt ook wanneer een leverancier van clouddiensten wordt ingeschakeld (bijv. externe gegevensopslag)[21].

Indien een app-ontwikkelaar derden toegang biedt tot gebruikersgegevens (zoals een advertentienetwerk dat toegang krijgt tot de geolocatiegegevens van het apparaat om gedragsgerichte reclame te kunnen aanbieden), moet de ontwikkelaar gebruikmaken van gepaste methoden om te voldoen aan de door de EU-wetgeving gestelde vereisten. Indien een derde toegang krijgt tot de op het apparaat opgeslagen gegevens, is artikel 5, lid 3, van de e-privacyrichtlijn van toepassing, op grond waarvan om geïnformeerde toestemming moet worden gevraagd. Als een derde partij bovendien persoonsgegevens voor eigen doeleinden verwerkt, kan hij samen met de app-ontwikkelaar als gemeenschappelijk voor de verwerking verantwoordelijke worden aangemerkt. In dat geval moet hij ervoor zorgen dat het beginsel van de beperking van verwerkingsdoeleinden en de beveiligingsverplichtingen in acht worden genomen [22] met betrekking tot dat deel van de verwerking waarvan hij de doeleinden en de methoden bepaalt. Aangezien er verschillende – zowel commerciële als technische – afspraken kunnen bestaan tussen app-ontwikkelaars en derden, zal de respectieve verantwoordelijkheid van elke partij per geval moeten worden vastgesteld, rekening houdend met de specifieke omstandigheden van de betreffende verwerking.

Een app-ontwikkelaar kan gebruikmaken van de bibliotheken van derden met software die gemeenschappelijke functionaliteit biedt, zoals bijvoorbeeld de bibliotheek voor een social gaming-platform. De app-ontwikkelaar moet ervoor zorgen dat gebruikers op de hoogte zijn van de eventuele verwerking van hun gegevens door dergelijke bibliotheken. Wanneer dit soort verwerking plaatsvindt, dient dit te gebeuren in overeenstemming met de EU-wetgeving, waar nodig ook door toestemming te vragen aan de gebruiker. In dit verband moeten app-ontwikkelaars vermijden om functionaliteit te gebruiken die voor de gebruiker verborgen blijven.

3.3.2 Fabrikanten van besturingssystemen en apparaten

De fabrikanten van besturingssystemen en apparaten dienen ook als voor de verwerking verantwoordelijken te worden beschouwd (en voor zover van toepassing als gemeenschappelijk verantwoordelijken) wanneer zij persoonsgegevens verwerken voor hun eigen doeleinden, zoals het soepel laten functioneren van het apparaat, de beveiliging, enz. Hiertoe behoren gegevens die door de

---

[21] Zie Advies 05/2012 van de Groep Artikel 29 over cloud computing (juli 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf.

[22] Zie Advies 2/2010 van de Groep artikel 29 over online reclame op basis van surfgedrag ('behavioural advertising') (juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf en Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker" (februari 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf.

gebruiker zijn geleverd (bijv. gebruikersgegevens bij registratie), automatisch door het apparaat aangemaakte gegevens (bijv. als het apparaat is uitgerust met een 'phone home'-functie die informatie doorgeeft over de locatie van het apparaat) of persoonsgegevens die door het besturingssysteem of de fabrikant van het apparaat worden verwerkt naar aanleiding van de installatie of het gebruik van apps. Wanneer de fabrikant van het besturingssysteem of het apparaat aanvullende functionaliteit aanbiedt, zoals de mogelijkheid om reservekopieën te maken of het apparaat op afstand te lokaliseren, zijn zij eveneens verantwoordelijk voor de verwerking van persoonsgegevens voor deze doeleinden.

Apps die geolocatiegegevens nodig hebben, zijn afhankelijk van de locatiediensten van het besturingssysteem. Wanneer een app gebruikmaakt van geolocatie, kan het besturingssysteem persoonsgegevens verzamelen om geolocatie-informatie te verstrekken aan de apps; de fabrikant kan ook overwegen om de gegevens te gebruiken om zijn eigen locatiediensten te verbeteren. In het laatste geval is de fabrikant van het besturingssysteem de voor de verwerking verantwoordelijke.

De fabrikanten van besturingssystemen en apparaten zijn ook verantwoordelijk voor de "application programming interface" (API), die apps in staat stelt persoonsgegevens op een intelligent apparaat te verwerken. De app-ontwikkelaar kan toegang krijgen tot gebruiksmogelijkheden en functies die de fabrikanten van besturingssystemen en apparaten beschikbaar stellen door middel van API's. Aangezien de fabrikanten bepalen op welke wijze (en in welke mate) toegang kan worden verkregen tot persoonsgegevens, moeten zij ervoor zorgen dat de toegang voor de app-ontwikkelaar voldoende schaalbaar is, d.w.z. dat hij alleen toegang krijgt tot de gegevens die noodzakelijk zijn voor het functioneren van de app. De fabrikanten van besturingssystemen en apparaten moeten er bovendien voor zorgen dat deze toegang op een eenvoudige en doeltreffende manier kan worden geblokkeerd.

Het begrip "ingebouwde privacybescherming" ("privacy by design") is een belangrijk beginsel waarnaar in de richtlijn gegevensbescherming al indirect wordt verwezen[23] en dat, samen met "standaardprivacybescherming" ("privacy by default"), duidelijker naar voren komt in de e-privacyrichtlijn[24]. Dit beginsel vereist van de fabrikanten van apparaten of applicaties dat zij de gegevensbescherming vanaf het allereerste begin in het ontwerp opnemen. Ingebouwde privacybescherming is een uitdrukkelijke voorwaarde bij het ontwerpen van telecommunicatieapparatuur, zoals bepaald in de richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur[25].

Fabrikanten van besturingssystemen en apparaten hebben derhalve, samen met app-winkels, een grote verantwoordelijkheid voor het waarborgen van de bescherming van de persoonsgegevens en de privacy van app-gebruikers. Dit omvat mede de verplichting om de beschikbaarheid te garanderen van procedures om de eindgebruiker te informeren en voor te lichten over de mogelijkheden van apps en de gegevens waartoe zij toegang kunnen krijgen, alsook om gebruikers geschikte instellingen te bieden waarmee zij de kenmerken van de verwerking kunnen aanpassen[26].

---

[23] Zie overweging 46 en artikel 17.

[24] Zie artikel 14, lid 3.

[25] Richtlijn 1999/5/EG van 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit. Publicatieblad van de Europese Gemeenschappen L 91 van 7.4.1999 blz. 10. Artikel 3, lid 3, onder c), bepaalt dat de Commissie kan besluiten dat apparatuur van eindgebruikers zo geconstrueerd moet zijn dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen.

[26] De werkgroep verheugt zich in dit verband over de aanbevelingen van de FTC, die bijvoorbeeld op pagina 15 van het in voetnoot 6 vermelde rapport over Mobiele Privacyvoorlichting stelt: *"(…) platforms bevinden zich in de unieke positie om samenhangende voorlichting te bieden in alle apps en worden hiertoe ook aangemoedigd. In lijn met de opmerkingen die tijdens de workshops zijn gemaakt, zouden zij ook kunnen overwegen dit op meerdere momenten te doen (…)."*

3.3.3 App-winkels

Elk van de meest gebruikte soorten intelligente apparaten heeft zijn eigen app-winkel. Niet zelden hebben bepaalde besturingssystemen nauwe banden met een specifieke app-winkel. App-winkels verwerken vaak betalingen voor de aanschaf van apps en kunnen ook ondersteuning bieden bij het verrichten van aankopen door middel van apps; gebruikers moeten zich daarom laten registreren met hun naam, adres en financiële gegevens. Deze (direct) identificeerbare gegevens kunnen worden gecombineerd met gegevens over aankoop- en gebruiksgedrag, alsook met gegevens die worden geraadpleegd in, of aangemaakt door het apparaat (zoals unieke identificatiegegevens). App-winkels kunnen waarschijnlijk worden aangemerkt als de verantwoordelijke voor de verwerking van dit soort persoonsgegevens, ook wanneer zij deze informatie terugsluizen naar de app-ontwikkelaars. Wanneer een app-winkel het downloaden van een app door een eindgebruiker, zijn gebruiksgeschiedenis of vergelijkbare informatie verwerkt om eerder gedownloade apps te herstellen, zijn zij ook verantwoordelijk voor de verwerking van persoonsgegevens voor dit doel.

App-winkels slaan inloggegevens op, evenals overzichten van eerder gekochte apps. Zij vragen gebruikers ook om hun creditcardgegevens, die samen met de overige accountgegevens van de klant worden bewaard. Bij dit soort transacties is de app-winkel de voor verwerking verantwoordelijke.

Websites die de mogelijkheid bieden om apps te downloaden en op het apparaat te installeren zonder dat authenticatie vereist is, kunnen er daarentegen van uitgaan dat zij geen persoonsgegevens verwerken.

App-winkels bevinden zich in een uitstekende positie om app-ontwikkelaars in staat te stellen gepaste informatie over de app te verstrekken, inclusief het soort gegevens dat de app kan verwerken en voor welke doeleinden. App-winkels kunnen deze normen handhaven door middel van hun toelatingsbeleid (gebaseerd op controles die hetzij vooraf, hetzij achteraf kunnen plaatsvinden). In samenwerking met de fabrikanten van besturingssystemen kunnen app-winkels een kader ontwikkelen dat app-ontwikkelaars in staat stelt samenhangende en begrijpelijke mededelingen te doen (bijvoorbeeld door middel van symbolen die een bepaald soort toegang tot sensorgegevens weergeven) en deze duidelijk zichtbaar op te nemen in de catalogus van de app-winkel.

3.3.4 Derden

Er zijn veel verschillende derden betrokken bij de verwerking van gegevens die voortvloeit uit het gebruik van apps.

Veel gratis apps worden bijvoorbeeld gefinancierd door middel van reclame, die kan bestaan uit, maar niet beperkt blijft tot contextgebonden of op de persoon toegesneden advertenties, die mogelijk worden gemaakt door trackingvoorzieningen als cookies of andere gegevens waarmee apparaten kunnen worden geïdentificeerd. De reclame kan bestaan uit een banner in de app, advertenties die buiten de app om worden aangeboden door de browserinstellingen aan te passen of iconen op het mobiele bureaublad te plaatsen of die worden aangeboden door de inhoud van de app te personaliseren (bijv. gesponsorde zoekresultaten).

Reclame voor apps wordt over het algemeen verzorgd door advertentienetwerken en gelijksoortige intermediairs die banden hebben met, of tot dezelfde organisatie behoren als fabrikanten van bestuurssystemen of app-winkels. Zoals beschreven in advies 2/2010 van de Groep artikel 29[27] gaat

[27] Zie Advies 2/2010 van de Groep artikel 29 over online reclame op basis van surfgedrag (‘behavioural advertising’) (juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf.

online reclame dikwijls gepaard met de verwerking van persoonsgegevens zoals gedefinieerd in artikel 2 van de richtlijn gegevensbescherming en geïnterpreteerd door de Groep artikel 29[28].

Andere voorbeelden van derden zijn de leveranciers van analyse- en communicatiediensten. Leveranciers van analysediensten stellen app-ontwikkelaars in staat om inzicht te krijgen in het gebruik, de populariteit en de bruikbaarheid van hun apps. Ook de leveranciers van communicatiediensten[29] kunnen een belangrijke rol spelen bij het bepalen van de standaardinstellingen en de beveiligingsupdates van veel apparaten en kunnen gegevens verwerken over het gebruik van apps. Hun merkspecifieke aanpassingen ("branding") kunnen gevolgen hebben voor de mogelijke technische en functionele maatregelen die de gebruiker kan toepassen om zijn of haar persoonsgegevens te beschermen.

Vergeleken met app-ontwikkelaars kunnen derden twee rollen vervullen: de eerste is om taken uit te voeren voor de app-eigenaar, bijvoorbeeld om analysegegevens in de app aan te maken. In dit geval, wanneer zij uitsluitend handelen namens de app-ontwikkelaar en geen gegevens voor hun eigen doeleinden verwerken en/of geen gegevens delen met meerdere ontwikkelaars, treden zij waarschijnlijk op als gegevensverwerkers.

De tweede rol is om informatie te verzamelen over meerdere apps met als doel aanvullende diensten te bieden: de levering van statistische gegevens ten behoeve van analyses op grotere schaal (populariteit van apps, persoonlijke aanbevelingen) of om te voorkomen dat dezelfde advertentie nogmaals aan dezelfde gebruiker wordt getoond. Wanneer derden persoonsgegevens voor hun eigen doeleinden verwerken, treden zij op als voor de verwerking verantwoordelijken en moeten zij derhalve voldoen aan alle toepasselijke bepalingen van de richtlijn gegevensbescherming[30].
In het geval van gedragsgerichte reclame moet de voor de verwerking verantwoordelijke geldige toestemming van de gebruiker krijgen om persoonsgegevens te verzamelen en te verwerken, bijvoorbeeld om persoonsgegevens te analyseren en te combineren, of profielen te creëren en/of toe te passen. Zoals al werd uitgelegd in advies 2/2010 van de Groep artikel 29 over online reclame op basis van surfgedrag, kan deze toestemming het beste worden verkregen door gebruik van een voorafgaande opt-inprocedure.

Een bedrijf levert statistische gegevens over gebruikersgedrag aan app-eigenaars en adverteerders met gebruikmaking van trackers die door de app-ontwikkelaar in apps worden ingebouwd. De trackers van het bedrijf kunnen derhalve in veel apps en op veel apparaten worden geïnstalleerd. Een van de geboden diensten bestaat uit het informeren van app-ontwikkelaars over de andere apps waarvan de gebruiker gebruikmaakt, waarvoor unieke identificatiegegevens worden verzameld. Het bedrijf bepaalt in dit geval de vorm (trackers) en de doeleinden van de ontwikkelde hulpmiddelen voordat hij deze aanbiedt aan app-ontwikkelaars, adverteerders en andere partijen. Hij treedt bijgevolg op als voor de verwerking verantwoordelijke.

Voor zover derden informatie op intelligente apparaten raadplegen of opslaan, moeten zij voldoen aan het toestemmingsvereiste van artikel 5, lid 3, van de e-privacyrichtlijn.

In dit verband is het belangrijk op te merken dat gebruikers bij intelligente apparaten over het algemeen slechts beperkte mogelijkheden hebben om software te installeren die de verwerking van persoonsgegevens beheert, iets wat op bureaucomputers gebruikelijk is. Als alternatief voor http-

---

[28] Zie ook de interpretatie van het begrip persoonsgegevens in Advies 4/2007 van de Groep artikel 29 over het begrip persoonsgegeven (juni 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf.

[29] De leveranciers van communicatiediensten zijn ook onderworpen aan branchespecifieke verplichtingen die buiten het bereik van dit advies vallen.

[30] Advies 2/2010 van de Groep artikel 29 over online reclame op basis van surfgedrag ('behavioural advertising'), blz. 10-11.

cookies raadplegen derden vaak unieke identificatiegegevens om (groepen) gebruikers te selecteren en deze gericht van diensten te voorzien, waaronder reclame. Aangezien veel van deze identificatiegegevens niet kunnen worden gewist of gewijzigd door de gebruiker (zoals IMEI, IMSI, MSISDN[31] en specifieke, unieke identificatiegegevens van het apparaat die door het besturingssysteem worden toegevoegd) hebben deze derden de mogelijkheid om aanzienlijke hoeveelheden persoonsgegevens te verwerken zonder dat de gebruiker hier invloed op heeft.

3.4 Rechtsgrondslag

Om persoonsgegevens te mogen verwerken, is een van de wettelijke gronden vereist die in artikel 7 van de richtlijn gegevensbescherming worden genoemd. Artikel 7 onderscheidt zes wettelijke gronden voor gegevensverwerking: de ondubbelzinnige toestemming van de betrokkene; noodzaak van de verwerking voor de uitvoering van een overeenkomst waarbij de betrokkene partij is; de bescherming van vitale belangen van de betrokkene; de naleving van een wettelijke verplichting; (in het geval van de overheid) de uitvoering van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag, en de behartiging van een gerechtvaardigd (bedrijfs)belang.

Met betrekking tot het opslaan van informatie of het verkrijgen van toegang tot informatie die al op het intelligente apparaat is opgeslagen, stelt artikel 5, lid 3, van de e-privacyrichtlijn een meer gedetailleerde afbakening/beperking vast van de wettelijke gronden die in acht moeten worden genomen.

3.4.1 Toestemming voorafgaand aan installatie en verwerking van persoonsgegevens

In het geval van apps is toestemming de voornaamste toepasselijke wettelijke grond. Wanneer een app wordt geïnstalleerd, wordt er informatie op het apparaat van de eindgebruiker geplaatst. Veel apps hebben toegang tot gegevens die op het apparaat zijn opgeslagen, waaronder de contacten in het adresboek, foto's, video's en andere persoonlijke documenten. In al deze gevallen is ingevolge artikel 5, lid 3, van de e-privacyrichtlijn toestemming van de gebruiker vereist, gebaseerd op duidelijke en volledige informatie, voordat de informatie op het apparaat kan worden geplaatst of opgevraagd.

Het is belangrijk om het onderscheid te beseffen tussen de toestemming die vereist is om informatie op het apparaat te plaatsen en te lezen, en toestemming als wettelijke grond voor de verwerking van verschillende soorten persoonsgegevens. Hoewel beide vormen van toestemming tegelijkertijd van toepassing zijn, elk gebaseerd op een verschillende rechtsgrondslag, geldt in beide gevallen de voorwaarde dat het hier om een vrije, specifieke en op informatie berustende wilsuiting moet gaan (zoals voorzien in artikel 2, onder h) van de richtlijn gegevensbescherming). Beide soorten toestemming kunnen derhalve in de praktijk worden samengevoegd, hetzij tijdens de installatie, hetzij voordat de app een aanvang maakt met de verzameling van persoonsgegevens op het apparaat, op voorwaarde dat de gebruiker er op ondubbelzinnige wijze op wordt gewezen waarmee hij instemt.

Veel app-winkels bieden app-ontwikkelaars de gelegenheid om eindgebruikers te informeren over de basiskenmerken van een app voordat zij deze installeren en vragen aan gebruikers om bepaalde stappen te nemen voordat zij de app kunnen downloaden en installeren (bijv. op de knop "installeren" drukken). Hoewel met dit soort stappen in sommige gevallen wordt voldaan aan het toestemmingsvereiste van artikel 5, lid 3, wordt hierbij waarschijnlijk te weinig informatie verstrekt om dit te kunnen aanmerken als geldige toestemming voor de verwerking van persoonsgegevens. Dit

[31] Mobile Station Integrated Services Digital Network.

thema werd eerder geanalyseerd in advies 15/2011 van de Groep artikel 29 over de definitie van toestemming[32].

In de context van intelligente apparaten betekent "vrije wilsuiting" dat een gebruiker de keuze moet hebben om de verwerking van zijn persoonsgegevens te accepteren of te weigeren. Als het derhalve nodig is dat een app persoonsgegevens verwerkt, dient de gebruiker vrij te zijn om dit te accepteren of te weigeren. De gebruiker mag niet geconfronteerd worden met een scherm waarop alleen de optie 'Ja, ik ga akkoord' staat vermeld om de installatie te kunnen voltooien. Ook de optie 'Annuleren' of een vergelijkbare optie om de installatie te onderbreken, moet beschikbaar zijn.

"Op informatie berustend" betekent dat de betrokkene de beschikking moet hebben over de noodzakelijke informatie om een gefundeerd oordeel te kunnen vormen[33]. Om eventuele dubbelzinnigheid te voorkomen, moet deze informatie worden aangeboden voordat er persoonsgegevens worden verwerkt. Dit omvat ook de verwerking van gegevens die plaatsvindt tijdens de installatie, bijvoorbeeld met het oog op de verwijdering van programmafouten ('debugging') en tracking. Op de inhoud en vorm van deze informatie wordt ingegaan in punt 3.7 van dit advies.

"Specifiek" betekent dat de wilsuiting betrekking moet hebben op de verwerking van concrete gegevens of een beperkte categorie van gegevensverwerking. Om deze reden kan het aanklikken van de knop "Installeren" niet als geldige toestemming worden beschouwd voor de verwerking van persoonsgegevens; de toestemming kan immers niet bestaan uit een algemeen geformuleerde machtiging. In sommige gevallen krijgen gebruikers de mogelijkheid om gespecificeerde toestemming te verstrekken, waarbij hun wordt gevraagd akkoord te gaan met ieder soort gegevens waartoe de app toegang wil verkrijgen[34]. Met een dergelijke aanpak wordt voldaan aan twee belangrijke wettelijke vereisten: ten eerste, om de gebruiker op toereikende wijze te informeren over belangrijke onderdelen van de dienst, en ten tweede, om hem te vragen specifieke toestemming voor elk onderdeel te geven[35]. De alternatieve aanpak, waarbij de app-ontwikkelaar de gebruikers verzoekt om akkoord te gaan met een lange reeks algemene voorwaarden en/of zijn privacybeleid, kan niet worden aangemerkt als specifieke toestemming[36].

Specifiek heeft ook betrekking op het bijhouden van gebruikersgedrag ('tracking') door adverteerders en andere derden. De standaardinstellingen van besturingssystemen en apps moeten erop gericht zijn om tracking te voorkomen en gebruikers de mogelijkheid te bieden specifieke toestemming te geven voor dit soort gegevensverwerking. Het moet voor derden niet mogelijk zijn deze standaardinstellingen te omzeilen, zoals momenteel vaak gebeurd met de opties voor "Niet volgen" die in browsers zijn opgenomen.

---

[32] Advies 15/2011 van de Groep artikel 29 over de definitie van toestemming (juli 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_nl.pdf.

[33] Idem, blz. 19.

[34] Gespecificeerde toestemming betekent dat gebruikers op gedetailleerde (gespecificeerde) wijze kunnen bepalen welke functies van de app die persoonsgegevens verwerkt, zij willen activeren.

[35] De noodzaak van gespecificeerde toestemming wordt ook nadrukkelijk bepleit door de FTC in haar meest recente rapport (zie noot 6) op blz. 15-16: *"(...) platformen zouden ook moeten overwegen 'just-in-time' informatie te bieden en uitdrukkelijke instemming te vragen met de verzameling van andere gegevens die veel consumenten in een ander verband als gevoelige informatie beschouwen, zoals foto's, contacten, kalenders, kalendernotities of audio- of video-opnamen*."

[36] Idem, blz. 34-35: *"Algemene toestemming zonder een exacte aanduiding van het doel van de verwerking waarmee de betrokkene akkoord gaat, voldoet niet aan dit vereiste. Dit betekent dat de informatie over het doel van de verwerking niet moet worden opgenomen in de algemene bepalingen, maar in een afzonderlijke toestemmingsclausule."*

Voorbeelden van specifieke toestemming

Een app biedt informatie over restaurants in de omgeving. Bij het installeren van de app moet de app-ontwikkelaar om toestemming vragen. Voor het gebruik van geolocatiegegevens moet de app-ontwikkelaar afzonderlijke toestemming vragen, d.w.z. tijdens de installatie of voordat de app toegang krijgt tot de geolocatie.
Specifiek betekent hier dat de toestemming beperkt moet blijven tot het specifieke gebruik van de gegevens om de gebruiker te informeren over nabijgelegen restaurants. De locatiegegevens uit het apparaat mogen derhalve alleen worden geraadpleegd wanneer de gebruiker de app voor dit concrete doel gebruikt. De toestemming van de gebruiker voor de verwerking van geolocatiegegevens betekent niet dat de app voortdurend locatiegegevens op het apparaat mag opvragen. Voor deze verdere verwerking is aanvullende informatie en afzonderlijke toestemming vereist.

Ook in het geval van een communicatie-app die toegang wil krijgen tot de contactenlijst, moet de gebruiker de mogelijkheid worden geboden de contacten te selecteren met wie hij wil communiceren, in plaats van toegang te verlenen tot het volledige adresboek (inclusief de contactgegevens van personen die geen gebruik maken van de betreffende dienst en die derhalve geen toestemming kunnen hebben gegeven voor de verwerking van gegevens die op hen betrekking hebben).

Het is echter belangrijk om op te merken dat zelfs wanneer de toestemming voldoet aan de drie genoemde criteria, dit geen vrijbrief is voor onredelijke en onrechtmatige verwerking. Indien het doel van de gegevensverwerking excessief en/of onevenredig is, mist deze een geldige rechtsgrondslag en is de verwerking vermoedelijk in strijd met de richtlijn gegevensbescherming, ook al heeft de gebruiker toestemming verleend.

Een voorbeeld van excessieve en onrechtmatige gegevensverwerking

Een wekker-app biedt de aanvullende optie om het alarm door middel van een gesproken commando uit te zetten of in de slaapstand te zetten. In dit voorbeeld zou de toestemming voor een eventuele geluidsopname alleen gelden zolang het alarm afgaat. Iedere registratie of opname van het geluid terwijl het alarm niet afgaat, zou waarschijnlijk worden aangemerkt als excessief en onrechtmatig.

In het geval van apps die standaard op het apparaat worden geïnstalleerd (voordat de eindgebruiker dit in zijn bezit krijgt) of van andere verwerkingen door het besturingssysteem waarvoor toestemming een wettelijk vereiste is, moeten de voor verwerking verantwoordelijken zorgvuldig beoordelen of deze toestemming werkelijk geldig is. In veel gevallen moet het gebruik van een afzonderlijke toestemmingsprocedure worden overwogen, wellicht wanneer de app voor het eerst wordt gebruikt, om de voor de verwerking verantwoordelijke voldoende gelegenheid te bieden om de eindgebruiker volledig te informeren. Wanneer gegevens behoren tot de bijzondere categorieën voorzien in artikel 8 van de richtlijn gegevensbescherming, moet toestemming uitdrukkelijk worden gegeven.

Niet in de laatste plaats moet gebruikers de gelegenheid worden geboden om hun toestemming op een eenvoudige en doeltreffende manier in te trekken. Hierop zal nader worden ingegaan in punt 3.8 van dit advies.

3.4.2 Rechtsgrondslag voor gegevensverwerking tijdens het gebruik van de app

Zoals hierboven werd aangegeven, is toestemming een noodzakelijke wettelijke voorwaarde als app-ontwikkelaars op rechtmatige wijze informatie willen plaatsen en/of raadplegen en bijgevolg persoonsgegevens willen verwerken. In een volgende fase, tijdens het gebruik van de app, kunnen app-ontwikkelaars andere wettelijke gronden aanvoeren voor andere soorten gegevensverwerking, zolang dit niet de verwerking van gevoelige persoonsgegevens betreft.

Deze wettelijke gronden kunnen bestaan uit de noodzaak van verwerking voor de uitvoering van een overeenkomst met de betrokkene of voor de behartiging van een gerechtvaardigd (bedrijfs)belang, zoals bepaald in artikel 7, onder b) en f), van de richtlijn gegevensbescherming.

Deze wettelijke gronden zijn beperkt tot de verwerking van niet-gevoelige persoonsgegevens van een specifieke gebruiker en kunnen alleen worden ingeroepen voor zover de verwerking van bepaalde gegevens strikt noodzakelijk is om de gewenste dienst te verlenen, of zoals in het geval van artikel 7, onder f), uitsluitend indien de bescherming van de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen dan de aangevoerde belangen.

Voorbeelden van contractuele vereisten als wettelijke grond

Een gebruiker geeft toestemming voor het installeren van een app voor mobiel bankieren. Om een betalingsopdracht uit te voeren, hoeft de bank geen afzonderlijke toestemming aan de gebruiker te vragen om zijn naam en rekeningnummer bekend te maken aan de ontvanger van de betaling. De verstrekking van de gegevens is strikt noodzakelijk voor de uitvoering van het contract met deze specifieke gebruiker en derhalve kan de bank zich baseren op de wettelijke grond van artikel 7, onder b), van de richtlijn gegevensbescherming. Dezelfde redenering geldt voor communicatie-apps: wanneer zij essentiële gegevens, zoals de naam van een account, een e-mailadres of een telefoonnummer aan iemand verstrekken met wie de gebruiker wil communiceren, is bekendmaking van de gegevens vanzelfsprekend noodzakelijk voor de uitvoering van het contract.

3.5 Doelbinding en minimale gegevensinzameling

De fundamentele beginselen waarop de richtlijn gegevensbescherming is gebaseerd, zijn doelbinding en minimale gegevensinzameling. Doelbinding stelt gebruikers in staat hun persoonsgegevens weloverwogen aan een ander toe te vertrouwen, aangezien zij te horen krijgen hoe hun gegevens zullen worden gebruikt en kunnen vertrouwen op de limitatieve opsomming van de verwerkingsdoeleinden die hen duidelijk maakt voor welke doeleinden hun gegevens zullen worden gebruikt. De doeleinden van de gegevensverwerking dienen derhalve duidelijk omschreven en begrijpelijk te zijn voor een gemiddelde gebruiker zonder gespecialiseerde juridische of technische kennis.

Doelbinding dwingt app-ontwikkelaars er bovendien toe hun bedrijfsmethoden goed te beoordelen voordat zij overgaan tot het verzamelen van gegevens van hun gebruikers. Persoonsgegevens mogen alleen worden verwerkt voor eerlijke en rechtmatige doeleinden (artikel 6, lid 1, onder a), van de richtlijn gegevensverwerking); deze doeleinden moeten worden vastgesteld voordat de verwerking van de gegevens plaatsvindt.

Doelbinding laat niet toe dat essentiële kenmerken van de verwerking plotseling worden gewijzigd.

Het oorspronkelijke doel van een app was bijvoorbeeld om gebruikers de mogelijkheid te bieden elkaar te e-mailen. De ontwikkelaar besluit echter zijn ondernemingsmodel te veranderen en voegt de e-mailadressen van zijn gebruikers samen met de telefoonnummers van de gebruikers van een andere app. De desbetreffende voor de verwerking verantwoordelijken zouden dan alle gebruikers persoonlijk moeten benaderen om hun voorafgaande ondubbelzinnige toestemming te vragen voor de verwerking van hun persoonsgegevens voor dit nieuwe doel.

Doelbinding hangt nauw samen met het beginsel van gegevensminimalisering. Om onnodige en mogelijk onrechtmatige gegevensverwerking te voorkomen, moeten app-ontwikkelaars zorgvuldig beoordelen welke gegevens strikt noodzakelijk zijn voor het gebruik van de gewenste functionaliteit.

Apps kunnen toegang krijgen tot veel van de functionaliteit op het apparaat en zijn derhalve tot veel in staat, zoals het sturen van heimelijke sms-berichten, het opzoeken van beelden en het raadplegen van het volledige adresboek. Veel app-winkels ondersteunen (semi)automatische updates waarmee de app-ontwikkelaar nieuwe gebruiksmogelijkheden in de app kan opnemen en beschikbaar kan stellen met weinig tot geen betrokkenheid van de eindgebruiker.

De werkgroep wil hier benadrukken dat derden die door middel van apps toegang verkrijgen tot gebruikersgegevens de beginselen van de beperking van verwerkingsdoeleinden en minimale gegevensinzameling in acht moeten nemen. De unieke, vaak onmogelijk te wijzigen identificatiegegevens van het apparaat horen niet te worden gebruikt ten behoeve van voorkeurgerichte reclame en/of analysediensten, omdat gebruikers hierbij niet de mogelijkheid hebben om hun toestemming in te trekken. App-ontwikkelaars moeten ervoor zorgen dat functieverschuiving wordt voorkomen door de verwerking in opeenvolgende versies van een app te veranderen zonder eindgebruikers hierover gepaste informatie te sturen en de gelegenheid te bieden zich aan de betreffende verwerking te onttrekken of de dienst geheel op te zeggen. Aan gebruikers moeten ook de technische middelen worden geboden om verklaringen over de aangevoerde doeleinden te verifiëren door hen toegang te bieden tot informatie over de hoeveelheid uitgaand dataverkeer per app in verhouding tot het door de gebruiker geïnitieerde verkeer.

Informatie en controle-instrumenten zijn essentiële gebruiksmogelijkheden om te garanderen dat de beginselen van minimale gegevensinzameling en de beperking van verwerkingsdoeleinden in acht worden genomen.

De toegang tot de onderliggende gegevens op het apparaat door middel van API's biedt fabrikanten van besturingssystemen en apparaten, alsook app-winkels, de gelegenheid om specifieke normen te handhaven en eindgebruikers gepaste informatie te bieden. Fabrikanten van besturingssystemen en apparaten zouden bijvoorbeeld een API moeten aanbieden met nauwkeurige bedieningsmogelijkheden waarmee onderscheid kan worden gemaakt tussen al dit soort gegevens om ervoor te zorgen dat app-ontwikkelaars alleen om toegang kunnen vragen tot die gegevens die strikt noodzakelijk zijn voor de (rechtmatige) toepassing van hun apps. Het soort gegevens waarom wordt verzocht door de app-ontwikkelaar kan dan duidelijk in de app-winkel worden vermeld om de gebruiker hierover te informeren voordat hij de app installeert.

In dit verband is de controle op de toegang tot de op het apparaat opgeslagen gegevens afhankelijk van verschillende mechanismen:

a. de fabrikanten van besturingssystemen en apparaten, evenals app-winkels stellen **normen** waaraan moet worden voldaan om te worden opgenomen in de winkels: app-ontwikkelaars moeten zich aan deze normen houden om niet het risico te lopen uitgesloten te worden van het assortiment[37];
b. de **API's** in besturingssystemen stellen standaardmethoden vast waarmee apps toegang kunnen krijgen tot de op een telefoon opgeslagen gegevens; deze hebben ook gevolgen voor de verzameling van gegevens van de kant van de server;
c. **controle vooraf** – controles die plaatsvinden voordat een app wordt geïnstalleerd[38];
d. **controle achteraf** – controles die worden uitgevoerd nadat een app is geïnstalleerd.

3.6 Beveiliging

Ingevolge artikel 17 van de richtlijn gegevensbescherming moeten voor de verwerking verantwoordelijken en verwerkers de noodzakelijke organisatorische en technische maatregelen treffen om de bescherming te garanderen van de persoonsgegevens die zij verwerken. Bijgevolg moeten alle partijen die in punt 3.3 worden onderscheiden maatregelen nemen overeenkomstig hun respectieve rol en verantwoordelijkheid.

---

[37] "Jailbroken" apparaten staan toe om apps buiten de officiële winkels om te installeren; apparaten met Android staan ook installatie uit andere bronnen toe.

[38] In het specifieke geval van voorgeïnstalleerde apps.

Het doel dat met de naleving van de beveiligingsverplichting wordt beoogd, is tweeledig. Het stelt gebruikers in staat het gebruik van hun gegevens strenger te controleren en tegelijkertijd wordt hiermee het vertrouwen vergroot in de entiteiten die de gegevens van de gebruikers daadwerkelijk verwerken.

Teneinde te voldoen aan hun respectieve beveiligingsverplichtingen als voor de verwerking verantwoordelijke, moeten app-ontwikkelaars, app-winkels, fabrikanten van besturingssystemen en apparaten, maar ook derden, rekening houden met de beginselen van ingebouwde privacybescherming en standaardprivacybescherming. Dit vergt een voortdurende beoordeling van zowel bestaande als toekomstige risico's op het gebied van gegevensbescherming, alsmede de invoering en evaluatie van doeltreffende risicobeperkende maatregelen, waaronder minimale gegevensinzameling.

App-ontwikkelaars

Er bestaan veel openbaar toegankelijke richtsnoeren betreffende de beveiliging van mobiele apps die zijn gepubliceerd door fabrikanten van besturingssystemen en apparaten, alsook door onafhankelijke derden, bijvoorbeeld ENISA[39].

Het valt buiten het bereik van dit advies om een overzicht te bieden van alle beveiligingspraktijken die worden toegepast bij de ontwikkeling van apps. De werkgroep wil echter deze gelegenheid aangrijpen om in te gaan op die praktijken die ernstige gevolgen kunnen hebben voor de grondrechten van gebruikers.

Een belangrijke beslissing voorafgaand aan het ontwerp van een app is waar gegevens zullen worden opgeslagen. In sommige gevallen worden gegevens op het apparaat opgeslagen, maar app-ontwikkelaars kunnen ook gebruikmaken van een client-servermodel. Dit betekent dat persoonsgegevens worden overgebracht of gekopieerd naar het systeem van de dienstenaanbieder. Opslag en verwerking van de gegevens op het apparaat biedt eindgebruikers de meeste controle over deze gegevens; het geeft hun bijvoorbeeld de mogelijkheid de gegevens te wissen als zij hun toestemming voor de verwerking besluiten in te trekken. De veilige opslag van gegevens op afstand kan echter nuttig zijn voor gegevensherstel na verlies of diefstal van een apparaat. Tussenoplossingen zijn ook mogelijk.

App-ontwikkelaars moeten een duidelijk beleid vaststellen voor de ontwikkeling en distributie van software. Er is ook een rol weggelegd voor de fabrikanten van besturingssystemen en apparaten bij de bevordering van veilige gegevensverwerking door apps, waarop hieronder wordt ingegaan. In de tweede plaats moeten app-ontwikkelaars en app-winkels een omgeving ontwerpen en implementeren die bevorderlijk is voor de veiligheid, inclusief hulpmiddelen die de verspreiding van schadelijke apps helpen voorkomen en het mogelijk maken om iedere app gemakkelijk te installeren/de-installeren.

Tot de goede praktijken die tijdens het ontwerp van een app kunnen worden toegepast, behoren de minimalisering van het aantal coderegels en de complexiteit daarvan, alsook de invoering van controles om te voorkomen dat gegevens ongewild worden overgedragen of in gevaar gebracht. Alle ingevoerde gegevens moeten bovendien worden gevalideerd om bufferoverloop of injectieaanvallen te voorkomen. Andere beveiligingsmechanismen die genoemd moeten worden, zijn goede strategieën voor het beheer van beveiligingspatches en de uitvoering van regelmatige, onafhankelijke beveiligingsinspecties. Daarnaast moet bij het ontwerpen van apps het beginsel worden toegepast van minimale autorisatie als standaardinstelling ("least privilege by default"), waardoor apps alleen toegang krijgen tot de gegevens die zij werkelijk nodig hebben om de gebruiker bepaalde

[39] ENISA "Smartphone Secure Development Guideline": http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines..

functionaliteit te bieden. App-ontwikkelaars en app-winkels zouden gebruikers ook door middel van waarschuwingen moeten aanmoedigen om deze goede ontwerppraktijken te complementeren met correcte gebruikspraktijken, zoals het actualiseren van apps aan de hand van de laatst beschikbare versie. Daarnaast kunnen zij hen eraan herinneringen dat het niet aan te raden is om dezelfde wachtwoorden voor verschillende diensten te gebruiken.

In de ontwerpfase van een app moeten app-ontwikkelaars ook maatregelen treffen ter voorkoming van ongeoorloofde toegang tot persoonsgegevens door ervoor te zorgen dat gegevens, voor zover nodig, zowel tijdens verzending als na opslag beschermd worden.

Mobiele apps dienen in specifieke delen van het geheugen van apparaten (sandbox[40]) te worden uitgevoerd om de negatieve effecten van schadelijke software/apps te beperken. App-ontwikkelaars moeten, in nauwe samenwerking met de fabrikanten van besturingssystemen en/of app-winkels, de beschikbare oplossingen benutten die gebruikers de mogelijkheid bieden om te zien welke gegevens worden verwerkt door welke apps en naar keuze autorisaties te activeren en deactiveren. Het gebruik van verborgen functionaliteit zou niet toegestaan mogen zijn.

App-ontwikkelaars moeten hun methoden voor authenticatie en de identificatie van gebruikers zorgvuldig beoordelen. Zij dienen geen permanente (apparaatgebonden) identificatiegegevens te gebruiken, maar in plaats daarvan app-gebonden of tijdelijke apparaatgebonden identificatiegegevens met een lage entropie, om te voorkomen dat gebruikers gedurende langere tijd worden gevolgd. Ook moet het gebruik van privacyvriendelijke procedures worden overwogen. Bij de authenticatie van gebruikers moeten app-ontwikkelaars bijzondere aandacht besteden aan het beheer van gebruikersnamen en wachtwoorden. Deze laatste moeten gecodeerd en veilig worden opgeslagen in de vorm van een gecodeerde hashwaarde met sleutel. Het beschikbaar stellen aan gebruikers van tests om de sterkte van de gekozen wachtwoorden te beoordelen is ook een nuttige manier om de keuze van betere wachtwoorden te stimuleren (entropiecontrole). Waar toepasselijk (bij toegang tot gevoelige gegevens, maar ook bij toegang tot betaalde informatie) kan meervoudige authenticatie worden overwogen, mede door gebruik van meerdere factoren en verschillende kanalen (bijv. een via sms toegezonden toegangscode), en/of het gebruik van authenticatiegegevens die aan de eindgebruiker gekoppeld zijn (in plaats van aan het apparaat). Bij het selecteren van sessie-identificatiegegevens moeten bovendien onvoorspelbare reeksen worden gebruikt, waar mogelijk in combinatie met contextgebonden informatie zoals datum en tijd, maar ook het IP-adres of geolocatiegegevens.

App-ontwikkelaars moeten ook acht slaan op de in de e-privacyrichtlijn gestelde eisen met betrekking tot inbreuken op persoonsgegevens en de noodzaak om gebruikers proactief te informeren. Hoewel deze eisen momenteel alleen gelden voor aanbieders van openbare elektronischecommunicatiediensten, zal deze verplichting naar verwachting worden uitgebreid naar alle voor de verwerking verantwoordelijken (en verwerkers) door de aanstaande Verordening gegevensbescherming zoals voorgesteld door de Commissie (COM 2012/0011/COD). Hierdoor wordt de noodzaak nog verder versterkt om over een degelijk, voortdurend bijgewerkt "beveiligingsplan" te beschikken betreffende de verzameling, opslag en verwerking van persoonsgegevens om te voorkomen dat dergelijke inbreuken plaatsvinden, alsook de zware geldboetes te vermijden waarin voor dit soort gevallen is voorzien. Het beveiligingsplan moet onder meer ook zorgen voor kwetsbaarheidsbeheer en het tijdig en veilig uitbrengen van betrouwbare bugfix-updates.

De verantwoordelijkheid van app-ontwikkelaars voor de veiligheid van hun producten houdt niet op bij de levering van een gebruikersversie aan de markt. De beveiliging van apps kan, net als ieder softwareproduct, gebreken en kwetsbare plekken vertonen; app-ontwikkelaars moeten daar

[40] Een "sandbox" (letterlijk zandbak) is een beveiligingsmechanisme dat programma's gescheiden laat uitvoeren.

oplossingen of patches voor ontwikkelen en deze aanbieden aan partijen die deze aan de gebruikers kunnen leveren (of deze zelf direct aan de gebruikers leveren).

App-winkels
App-winkels zijn een belangrijke intermediair tussen eindgebruikers en app-ontwikkelaars en dienen apps te onderwerpen aan een aantal degelijke en doeltreffende controles voordat zij deze op de markt toelaten. Zij moeten informatie verstrekken over de controles die zij daadwerkelijk uitvoeren, onder meer over het soort controles dat zij uitvoeren om te beoordelen of aan de gegevensbescherming wordt voldaan.

Hoewel deze maatregelen niet 100 % effectief zijn ter voorkoming van de verspreiding van schadelijke apps, blijkt uit de statistieken dat deze aanpak zorgt voor een forse daling van de hoeveelheid schadelijke functionaliteit in producten uit "officiële" app-winkels[41].
Gezien het grote aantal apps dat dagelijks wordt aangeleverd, zou dit proces gebaat zijn bij de beschikbaarheid van automatische analyseprogramma's, alsook de creatie van kanalen voor de uitwisseling van informatie tussen beveiligings- en softwaredeskundigen, en de invoering van doeltreffende procedures en beleidsmaatregelen voor de afhandeling van gemelde problemen.

Behalve aan controles voorafgaand aan toelating tot de app-winkel, dienen apps ook te worden onderworpen aan openbare beoordelingsmechanismen. Gebruikers zouden daarbij niet alleen moeten beoordelen hoe "cool" een app is, maar ook een oordeel geven over de functionaliteit daarvan, in het bijzonder de kwaliteit van de privacybescherming en de beveiliging. Deze beoordelingsmechanismen moeten bovendien zodanig zijn opgezet dat valse beoordelingen worden voorkomen. Waarderings- en beoordelingsmechanismen voor apps kunnen ook bijdragen aan het wederzijds vertrouwen tussen de verschillende betrokken organisaties, met name als gegevens worden uitgewisseld via een lange keten van derden.

App-winkels hanteren vaak een methode om schadelijke of onveilige apps op afstand te kunnen de-installeren. Als dit mechanisme echter niet goed ontworpen is, kan het een beletsel vormen om gebruikers meer controle over hun gegevens te bieden. Als een app-winkel apps op een privacyvriendelijke manier op afstand wil de-installeren, dient dit te gebeuren op basis van goede informatie en de instemming van de klant. Bovendien moeten, vanuit een meer praktisch oogpunt, aan gebruikers kanalen worden geboden om feedback te geven op beveiligingsproblemen met hun apps en de doeltreffendheid van eventuele procedures voor verwijdering op afstand.

Evenals app-ontwikkelaars moeten app-winkels op de hoogte zijn van hun toekomstige verplichtingen met betrekking tot de melding van inbreuken op persoonsgegevens en nauw samenwerken met app-ontwikkelaars om deze inbreuken te voorkomen.

Fabrikanten van besturingssystemen en apparaten
De fabrikanten van besturingssystemen en apparaten spelen ook een belangrijke rol bij het vaststellen van minimumnormen en beste praktijken voor app-ontwikkelaars, niet alleen met betrekking tot de veiligheid van de onderliggende software en API's, maar ook tot de hulpmiddelen, de ondersteuning en het documentatiemateriaal die zij bieden. Fabrikanten van besturingssystemen en apparaten dienen sterke en bekende coderingsalgoritmes beschikbaar te stellen en een passende sleutellengte te ondersteunen. Zij moeten ook sterke en veilige authenticatiemechanismen beschikbaar stellen aan app-ontwikkelaars (bijv. het gebruik van certificaten gewaarmerkt door erkende certificaatautoriteiten om te verifiëren of een gegevensbron op afstand geautoriseerd is). Hiermee kan ook worden voorkomen

[41] *"Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets"*, Y Zhou et al., Network and Distributed System Security Symposium (NDSS) 2012.

dat app-ontwikkelaars hun eigen authenticatiemechanismen moeten ontwikkelen. In de praktijk worden deze mechanismen vaak slecht geïmplementeerd, wat tot grote kwetsbaarheid leidt[42].

De toegang tot, en de verwerking van persoonsgegevens door apps dient te zijn geregeld met in API's verwerkte klassen en methoden die gepaste controles en waarborgen bieden. De fabrikanten van besturingssystemen en apparaten moeten ervoor zorgen dat de methoden en functies die toegang bieden tot persoonsgegevens de mogelijkheid bieden tot verwerking van verzoeken om gespecificeerde toestemming. Daarnaast moeten er ook stappen worden ondernomen om te voorkomen of te beperken dat toegang tot persoonsgegevens wordt verkregen door het gebruik van basale functies of andere methoden waarmee de controles en waarborgen in API's kunnen worden omzeild.

Fabrikanten van besturingssystemen en apparaten moeten ook duidelijke logbestanden ontwikkelen waarmee eindgebruikers een goed inzicht kunnen krijgen in de apps die toegang hebben verkregen tot de gegevens op hun apparaat.

Alle partijen moeten tijdig reageren op de ontdekking van kwetsbare plekken in de beveiliging zodat eindgebruikers niet onnodig worden blootgesteld aan beveiligingsgebreken. Helaas bieden sommige fabrikanten van besturingssystemen en apparaten (alsook telecommunicatiebedrijven wanneer zij apparaten onder eigen merk distribueren) geen ondersteuning op lange termijn aan de versies van het besturingssysteem, waardoor gebruikers niet langer beschermd zijn tegen bekende beveiligingsrisico's. Fabrikanten van besturingssystemen en apparaten moeten eindgebruikers samen met app-ontwikkelaars van tevoren informatie verstrekken over hoe lang zij regelmatige beveiligingsupdates zullen ontvangen. Zij dienen gebruikers ook zo snel mogelijk op de hoogte te stellen als zij een update nodig hebben om een beveiligingsprobleem te verhelpen.

Derden
De bovenstaande beveiligingkenmerken en -overwegingen moeten ook worden gehanteerd door derden wanneer zij persoonsgegevens verzamelen en verwerken voor hun eigen doeleinden, met name door adverteerders en de leveranciers van analysediensten. Dit omvat mede de veilige verzending en gecodeerde opslag van de unieke identificatiegegevens van het apparaat en de app-gebruiker, alsook van andere persoonsgegevens.

3.7 Informatie

3.7.1 Informatieplicht en vereiste inhoud

Volgens artikel 10 van de richtlijn gegevensbescherming heeft iedere betrokkene recht te worden geïnformeerd over de identiteit van de partij die verantwoordelijk is voor de verwerking van zijn persoonlijke gegevens. Met betrekking tot apps heeft de eindgebruiker bovendien het recht te worden geïnformeerd over het soort persoonsgegevens dat wordt verwerkt en het doel waarvoor de gegevens zijn bestemd. Als de persoonsgegevens van de gebruiker worden verzameld bij andere partijen in de app-sector (zoals beschreven in punt 3.3 van dit advies), heeft de eindgebruiker niettemin volgens artikel 11 van de richtlijn gegevensbescherming het recht om te worden geïnformeerd over deze gegevensverwerking, op dezelfde wijze als hierboven aangegeven. Derhalve, wanneer hij persoonsgegevens verwerkt, moet de voor de verwerking verantwoordelijke de potentiële gebruikers ten minste informeren over:

---

[42] Er is recentelijk op gewezen dat het gebrek aan visuele beveiligingssignalen bij het gebruik van SSL/TLS en het ondeugdelijke gebruik van SSL/TLS kan worden benut om man-in-the-middle (MITM)-aanvallen te plegen. De totale gebruikersgroep die apps heeft geïnstalleerd, waarvan bewezen is dat deze kwetsbaar zijn voor MITM-aanvallen, bedraagt volgens recent onderzoek meerdere miljoenen personen. "*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security"*, Bernd Freisleben and Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

- wie hij is (naam en contactgegevens);
- de exacte categorieën persoonsgegevens die de app-ontwikkelaar zal verzamelen en verwerken;
- waarom de gegevensverwerking noodzakelijk is (voor welke doeleinden);
- of er gegevens zullen worden doorgegeven aan derden;
- welke rechten gebruikers hebben, zoals het intrekken van toestemming en het wissen van gegevens.

De verstrekking van deze informatie over gegevensverwerking is essentieel om toestemming te krijgen van de gebruiker voor de verwerking van de gegevens. De toestemming kan alleen geldig zijn als de betrokkene eerst is geïnformeerd over de belangrijkste aspecten van de gegevensverwerking. Het verstrekken van deze informatie nadat de app al is begonnen persoonsgegevens te verwerken (vaak al tijdens de installatie) kan niet als toereikend worden beschouwd en is derhalve niet rechtsgeldig. In lijn met het rapport van de Federal Trade Commission benadrukt de werkgroep de noodzaak om informatie te verstrekken op het moment dat deze voor consumenten van belang is, te weten net voordat deze informatie door apps wordt verzameld. Het ontvangen van informatie over welke gegevens worden verwerkt, is met name van belang vanwege de hoge mate van toegang die apps hebben tot sensoren en gegevensstructuren in het apparaat, terwijl deze toegang in veel gevallen niet vanzelfsprekend is. Gepaste informatie is ook van wezenlijk belang wanneer de app speciale categorieën persoonsgegevens verwerkt, bijv. betreffende iemands gezondheidstoestand, politieke overtuigingen, seksuele geaardheid, enz. De app-ontwikkelaar moet ten slotte een duidelijk onderscheid maken tussen verplichte en optionele informatie; het systeem moet de gebruiker daarbij de mogelijkheid bieden de toegang tot optionele informatie te weigeren met privacyvriendelijke standaardopties.

Met betrekking tot de identiteit van de voor de verwerking verantwoordelijke dienen gebruikers te weten wie wettelijk aansprakelijk is voor de verwerking van hun persoonsgegevens en hoe zij die partij kunnen bereiken. Zonder deze informatie kunnen zij hun rechten niet uitoefenen, zoals het recht om (op afstand) inzage te krijgen in hun opgeslagen persoonsgegevens. Aangezien de app-sector zeer gefragmenteerd is, is het essentieel dat iedere app over een eigen contactorganisatie beschikt, die verantwoording neemt voor alle gegevensverwerking die via de app plaatsvindt. Het kan niet van de eindgebruiker worden verwacht dat hij de betrekkingen onderzoekt tussen de app-ontwikkelaar en andere derden die door middel van de app persoonsgegevens verwerken.

Met betrekking tot het (de) beoogde doel(einden) moeten eindgebruikers op gepaste wijze worden geïnformeerd over de persoonsgegevens die worden verzameld en waarom. Gebruikers moeten er ook in duidelijke, begrijpelijke bewoordingen op worden gewezen of de gegevens door andere partijen opnieuw kunnen worden gebruikt, en zo ja, voor welke doeleinden. Rekbare doeleinden zoals ‘productvernieuwing’ zijn niet toereikend om gebruikers te informeren. Het moet duidelijk worden aangegeven of gebruikers worden verzocht toestemming te geven voor het delen van de informatie met derden ten behoeve van reclame- en/of analysedoeleinden. App-winkels hebben een grote verantwoordelijkheid om ervoor te zorgen dat deze informatie voor iedere app beschikbaar en gemakkelijk toegankelijk is.

App-winkels hebben een grote verantwoordelijkheid bij de verstrekking van gepaste informatie. Het gebruik van visuele aanduidingen of iconen die aangeven welk gebruik er van gegevens kan worden gemaakt, wordt sterk aanbevolen om gebruikers te informeren over de verschillende soorten gegevensverwerking.

Met het oog op de redelijke verwerking van persoonsgegevens adviseert de werkgroep dat voor de verwerking verantwoordelijken naast de bovengenoemde minimumgegevens, noodzakelijk om toestemming te krijgen van de app-gebruiker, gebruikers ook informatie verstrekken over:

- de evenredigheidscriteria voor de verschillende soorten gegevens die op het apparaat worden verzameld of geraadpleegd;

- de bewaartermijnen van de gegevens;
- de beveiligingsmaatregelen die de voor de verwerking verantwoordelijke toepast.

De werkgroep adviseert app-ontwikkelaars ook om in hun privacybeleid voor Europese gebruikers informatie op te nemen over op welke wijze wordt voldaan aan de Europese wetgeving op het gebied van gegevensbescherming, inclusief de mogelijke overdracht van persoonsgegevens vanuit Europa naar bijvoorbeeld de Verenigde Staten, en of (alsook hoe) in dat geval wordt voldaan aan de gemeenschappelijke veiligehavenbeginselen.

3.7.2 De vorm van verstrekking

De essentiële informatie over de verwerking van persoonsgegevens moet aan de gebruikers via de app-winkel worden aangeboden voordat zij de app installeren. In de tweede plaats moet de relevante informatie over de gegevensverwerking ook na installatie vanuit de app kunnen worden geraadpleegd.

Als partij die samen met de app-ontwikkelaars gezamenlijk verantwoordelijk is voor de informatieverstrekking, moeten app-winkels ervoor zorgen dat iedere app de essentiële informatie biedt over de verwerking van persoonsgegevens. Zij dienen de hyperlinks naar pagina's met privacy-informatie te controleren en apps te verwijderen waarin de links onbruikbaar zijn of de informatie over gegevensverwerking om andere redenen niet toegankelijk is.

De werkgroep adviseert om informatie over de verwerking van persoonsgegevens ook buiten de apps beschikbaar te stellen op gemakkelijk te vinden locaties, zoals in de app-winkel en bij voorkeur ook op de algemene websites van de app-ontwikkelaar die verantwoordelijk is voor de app. Het is onaanvaardbaar dat gebruikers in een positie worden gebracht waarin zij op internet informatie moeten gaan zoeken over het beleid van de app-ontwikkelaar betreffende de verwerking van gegevens en niet direct worden geïnformeerd door de app-ontwikkelaar of een andere voor de verwerking verantwoordelijke.

Op zijn minst dient iedere app leesbare, begrijpelijke en gemakkelijk toegankelijke informatie over het privacybeleid te bevatten, waarin al de bovengenoemde gegevens zijn opgenomen. Veel apps voldoen niet aan dit minimumvereiste voor transparantie. Volgens het onderzoek van FPF uit juni 2012 beschikt 56 % van de betaalde apps niet over een privacybeleid, evenmin als 30 % van de gratis apps.

Apps die geen persoonsgegevens verwerken, noch dit beogen, dienen dit duidelijk te vermelden in het privacybeleid.

Natuurlijk is de hoeveelheid informatie die kan worden weergegeven op een klein schermpje beperkt, maar dit mag geen excuus zijn om eindgebruikers niet op gepaste wijze te informeren. Er kunnen diverse strategieën worden gevolgd om gebruikers bekend te maken met de belangrijkste aspecten van de dienstverlening. Volgens de werkgroep kan het gebruik van getrapte meldingen, zoals beschreven in advies 10/2004 van de Groep artikel 29, nuttig zijn[43]. Hierbij bevat de aanvankelijke melding aan de gebruiker de minimuminformatie die vereist is door de EU-wetgeving; nadere informatie kan worden verkregen via koppelingen naar het volledige privacybeleid. De informatie moet direct op het scherm worden weergegeven, in een gemakkelijk toegankelijke en duidelijk zichtbare vorm. Naast de weergave van volledige informatie die geschikt is voor kleine schermen van mobiele apparaten, moeten gebruikers kunnen doorklikken naar een meer uitgebreide toelichting, bijvoorbeeld de tekst van het privacybeleid, waarin wordt uitgelegd hoe de app persoonsgegevens gebruikt, wie de voor de verwerking verantwoordelijke is en waar de gebruiker zijn rechten kan uitoefenen.

---

[43] Advies 10/2004 van de Groep artikel 29 over meer geharmoniseerde bepalingen inzake informatieverstrekking (juli 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_nl.pdf.

Deze aanpak kan worden gecombineerd met het gebruik van iconen, beelden, video en audio, alsook van contextgebonden real-time meldingen op het moment dat een app toegang zoekt tot het adresboek of foto's[44]. Deze iconen moeten begrijpelijk zijn, d.w.z. duidelijk, voor zichzelf sprekend en ondubbelzinnig. Het is duidelijk dat de fabrikant van het besturingssysteem een belangrijke gedeelde verantwoordelijkheid heeft om het gebruik van dergelijke iconen te vergemakkelijken.

App-ontwikkelaars zijn buitengewoon vaardig in het programmeren en ontwerpen van complexe interfaces voor kleine schermpjes en de werkgroep roept de sector daarom op dit creatieve talent te benutten om meer innovatieve oplossingen te ontwikkelen om gebruikers op mobiele apparaten op effectieve wijze te informeren. Om te garanderen dat de informatie werkelijk te begrijpen valt voor gebruikers zonder technische of juridische achtergrond, pleit de werkgroep (in lijn met het rapport van de FTC) er ten stelligste voor consumententesten te laten uitvoeren voor de gekozen informatiestrategieën[45].

3.8 De rechten van de betrokkene

Ingevolge artikel 12 en 14 van de richtlijn gegevensbescherming moeten app-ontwikkelaars en andere voor de verwerking verantwoordelijken in de app-sector, app-gebruikers in staat stellen om hun recht op toegang, rectificatie en verwijdering van hun persoonsgegevens uit te oefenen, alsook hun recht om bezwaar te maken tegen verwerking. Indien een gebruiker zijn recht op toegang uitoefent, dient de voor de verwerking verantwoordelijke de gebruiker informatie te verstrekken over de gegevens die worden verwerkt en de herkomst van die gegevens. Als een voor de verwerking verantwoordelijke geautomatiseerde besluiten neemt op basis van de verzamelde gegevens, moet deze de gebruiker ook informeren over de achterliggende logica van deze besluiten. Dit kan het geval zijn als de prestaties of het gedrag van gebruikers wordt beoordeeld, bijvoorbeeld op grond van financiële of gezondheidsgegevens, of van andere profielgegevens. Op verzoek van de gebruiker moet de voor de verwerking verantwoordelijke ook gelegenheid bieden tot rectificatie, verwijdering of blokkering van persoonsgegevens als deze onvolledig, onjuist of onrechtmatig verwerkt zijn.

Om gebruikers in staat te stellen controle uit te oefenen op de verwerking van hun persoonsgegevens moeten apps hun gebruikers op duidelijke en zichtbare wijze informeren over het bestaan van deze toegangs- en correctiemechanismen. De Groep artikel 29 adviseert om eenvoudige, maar veilige online toegangsinstrumenten te ontwerpen en te implementeren. Toegangsinstrumenten dienen bij voorkeur beschikbaar te zijn in iedere app, of anders via een koppeling naar een online toepassing, waar gebruikers direct toegang kunnen krijgen tot al hun gegevens die worden verwerkt en de noodzakelijke verklaring voor deze verwerking. Vergelijkbare initiatieven zijn al eerder ontwikkeld door online dienstenaanbieders, die bijvoorbeeld verschillende soorten controlepanelen of andere toegangsmechanismen beschikbaar hebben gesteld.

De behoefte aan soepele online toegang is vooral groot bij apps die uitvoerige gebruikersprofielen verwerken, zoals netwerk-apps, sociale apps en messaging-apps, alsook bij apps die gevoelige of financiële gegevens verwerken. Natuurlijk kan toegang alleen worden verleend als de identiteit van de betrokkene is vastgesteld, teneinde te voorkomen dat gegevens weglekken naar derden. Deze verplichting om te verifiëren of de identiteit correct is, moet echter niet leiden tot verder, overmatig verzamelen van persoonsgegevens van de betrokkene. In veel gevallen kan met authenticatie, in plaats van (volledige) identificatie, worden volstaan.

---

[44] Bijvoorbeeld het waarschuwingsicoontje op iPhones dat aangeeft dat geolocatieverwerking plaatsvindt.
[45] FTC-rapport, noot 6, blz. 16.

Daarnaast moet gebruikers altijd de mogelijkheid worden geboden hun toestemming op eenvoudige, niet bezwaarlijke wijze in te trekken. Een betrokkene kan zijn toestemming voor gegevensverwerking op verschillende manieren intrekken, alsook om verschillende redenen. Bij voorkeur dient de mogelijkheid tot het intrekken van toestemming te worden geboden door middel van de bovengenoemde gemakkelijk toegankelijke mechanismen. Het moet mogelijk zijn apps te de-installeren en zo alle persoonsgegevens te verwijderen, ook van de servers van de voor de verwerking verantwoordelijke. Om gebruikers de mogelijkheid te bieden hun gegevens te laten verwijderen door de app-ontwikkelaar, is er een belangrijke rol weggelegd voor de fabrikant van het besturingssysteem, die een melding aan de app-ontwikkelaar kan sturen wanneer een gebruiker de app de-installeert. Een dergelijke melding kan worden verstuurd via de API. In principe, zodra de gebruikers de app heeft gede-installeerd, heeft de app-ontwikkelaar geen wettelijke grond meer om de persoonsgegevens van die gebruiker te blijven verwerken, en is hij derhalve verplicht alle gegevens te wissen. Indien een app-ontwikkelaar bepaalde gegevens wenst te bewaren, bijvoorbeeld om herinstallatie van de app te vergemakkelijken, moet hij hiervoor toestemming vragen tijdens het de-installatieproces en de gebruiker vragen of hij akkoord gaat met een concrete aanvullende bewaartermijn. De enige uitzondering op deze regel is het bestaan van eventuele wettelijke verplichtingen om gegevens voor specifieke doeleinden te bewaren, bijvoorbeeld fiscale verplichtingen met betrekking tot financiële transacties[46].

3.9 Bewaartermijnen

App-ontwikkelaars moeten beoordelen hoe lang zij verzamelde gegevens kunnen bewaren en welke risico's dit oplevert op het gebied van gegevensbescherming. De specifieke termijnen zullen afhangen van het doel van de app en het belang van de gegevens voor de eindgebruiker. Bijvoorbeeld, in het geval van een kalender, een dagboek of een app voor het delen van foto's zal de bewaartermijn moeten worden bepaald door de eindgebruiker, terwijl het bij een navigatie-app voldoende kan zijn om de laatste 10 bezochte locaties op te slaan. App-ontwikkelaars moeten ook besluiten wat zij doen met de gegevens van gebruikers die hun app gedurende langere tijd niet hebben gebruikt. Deze gebruikers hebben mogelijk hun mobiele apparaat verloren of kunnen overgestapt zijn op een ander apparaat zonder de apps op het eerste apparaat te de-installeren. App-ontwikkelaars dienen daarom van tevoren een periode van inactiviteit vast te stellen, waarna de account als verlopen zal worden beschouwd. De gebruiker moet over de aangehouden termijn worden geïnformeerd. Wanneer deze termijn afloopt, moet de voor de verwerking verantwoordelijke de gebruiker waarschuwen en deze de gelegenheid bieden diens persoonsgegevens veilig te stellen. Indien de gebruiker niet op deze waarschuwing reageert, moeten de persoonsgegevens die betrekking hebben op de gebruiker en het gebruik van de app onherroepelijk worden geanonimiseerd of gewist. De periode waarna de waarschuwing wordt verstuurd, zal afhangen van het doel van de app en de locatie waar de gegevens zijn opgeslagen. Als het gegevens betreft die op het apparaat zelf zijn opgeslagen, bijvoorbeeld de hoogste score bij een spel, kunnen de gegevens zo lang worden bewaard als de app is geïnstalleerd. Als het gegevens zijn die slechts één keer per jaar worden gebruikt, zoals informatie over een skioord, kan de waarschuwing worden verstuurd na 15 maanden inactiviteit.

---

[46] De werkgroep herinnert alle diensten van de informatiemaatschappij, zoals apps, eraan dat de Europese verplichting tot het bewaren van gegevens (Richtlijn 2006/24/EG) niet op hen van toepassing is en derhalve niet kan worden ingeroepen als grond om gegevens van app-gebruikers te blijven verwerken nadat zij de app hebben verwijderd. De werkgroep grijpt de gelegenheid aan om te wijzen op de bijzonder riskante aard van verkeersgegevens, waarvoor op zich al bijzondere voorzorgsmaatregelen en waarborgen moeten worden getroffen – zoals benadrukt in het verslag van de Groep artikel 29 over de handhaving van de Richtlijn gegevensbewaring (WP172), waarin alle betrokken belanghebbenden werden opgeroepen gepaste beveiligingsmaatregelen te treffen.

3.10 Kinderen

Kinderen maken gretig gebruik van apps, hetzij op hun eigen apparaten, hetzij op apparaten die zij delen met anderen (bijv. die van hun ouders, broers of zussen, of apparaten op school), en er bestaat onmiskenbaar een grote en gevarieerde markt voor apps die voor kinderen zijn bestemd. Tegelijkertijd hebben kinderen echter weinig of geen besef, noch kennis, van de hoeveelheid gegevens en de gevoeligheid daarvan waartoe apps toegang kunnen krijgen, of de mate waarin gegevens worden gedeeld met derden voor reclamedoeleinden.

De werkgroep is uitgebreid ingegaan op het thema van de verwerking van de gegevens van kinderen in advies 2/2009 over de bescherming van persoonsgegevens van kinderen. Wij zullen hier derhalve alleen een aantal risico's bespreken en aanbevelingen formuleren die specifiek zijn voor apps[47].

App-ontwikkelaars en andere voor verwerking verantwoordelijken dienen goed te letten op de leeftijdsgrenzen die worden gesteld aan kinderen of minderjarigen in de wetgeving van landen waar ouderlijke toestemming een voorwaarde is voor de rechtmatige gegevensverwerking door apps[48].

Wanneer een minderjarige wettelijk toestemming kan verlenen en de app bedoeld is om te worden gebruikt door een kind of minderjarige, moet de voor de verwerking verantwoordelijke zich bewust zijn van diens mogelijk beperkte begripsvermogen en de beperkte aandacht die hij zal besteden aan informatie over gegevensverwerking. Vanwege hun algemene kwetsbaarheid, en gelet op het feit dat persoonsgegevens op eerlijke en rechtmatige wijze moeten worden verwerkt, moeten verantwoordelijken voor de verwerking van de gegevens van kinderen de beginselen van minimale gegevensinzameling en de beperking van verwerkingsdoeleinden nog strikter toepassen. Met name mogen de voor verwerking verantwoordelijken de gegevens van kinderen niet gebruiken voor gedragsgerichte reclame, direct noch indirect, aangezien dit het begripsvermogen van kinderen te boven gaat en derhalve de grenzen van rechtmatige verwerking overschrijdt.

De werkgroep deelt in dit verband de zorgen die door de Federal Trade Commission worden geuit in haar rapport over mobiele apps voor kinderen[49].

App-ontwikkelaars dienen, in samenwerking met app-winkels en de fabrikanten van besturingssystemen en apparaten, de relevante informatie op een eenvoudige manier weer te geven, rekening houdend met de leeftijd van de gebruiker. De voor de verwerking verantwoordelijken moeten zich er bovendien specifiek van onthouden gegevens te verzamelen over de ouders of gezinsleden van kinderen die apps gebruiken, zoals financiële informatie of informatie over specifieke categorieën gegevens, bijvoorbeeld medische gegevens.

4 Conclusies en aanbevelingen

Veel van de gegevens die zich op een intelligent mobiel apparaat bevinden, zijn persoonsgegevens. Het toepasselijke juridische kader wordt gevormd door de richtlijn gegevensbescherming, in combinatie met het toestemmingsvereiste vermeld in artikel 5, lid 3, van de e-privacyrichtlijn. Deze

---

[47] WP 160, Advies 2/2009 over de bescherming van persoonsgegevens van kinderen (Algemene richtlijnen en het bijzondere geval van scholen) (11 februari 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_nl.pdf.

[48] In de EU-lidstaten lopen de leeftijdsgrenzen uiteen van 12 tot 18 jaar.

[49] FTC-rapport Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (februari 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. "*Hoewel de Commission een zeer gevarieerd aanbod aantrof van apps voor kinderen die door honderden verschillende ontwikkelaars waren gecreëerd, vond de Commission weinig tot geen informatie op de app-markt over de verzameling van gegevens en de wijze waarop apps deze in de praktijk delen*."

regels zijn van toepassing op iedere app bestemd voor app-gebruikers in de Unie, ongeacht de locatie van de app-ontwikkelaar of de app-winkel.

Het gefragmenteerde karakter van de app-sector, het grote aantal technische mogelijkheden om toegang te krijgen tot gegevens die op mobiele apparaten opgeslagen zijn of daarop aangemaakt worden, en het gebrek aan juridische kennis bij ontwikkelaars leveren een aantal ernstige risico's op voor de gegevensbescherming van app-gebruikers. Deze risico's variëren van een gebrek aan transparantie en een gebrek aan bewustzijn onder gebruikers tot tekortschietende beveiligingsmaatregelen, ongeldige toestemmingsprocedures, een trend naar de maximale inzameling van gegevens en de rekbaarheid van de doeleinden waarvoor gegevens worden verwerkt.

De verantwoordelijkheden van de verschillende partijen die betrokken zijn bij de ontwikkeling, distributie en exploitatie van apps overlappen elkaar. Het merendeel van de conclusies en aanbevelingen is bestemd voor de ontwikkelaars van apps (aangezien zij de meeste invloed hebben op de exacte wijze waarop de verwerking plaatsvindt of de informatie in de app wordt weergegeven). Om te kunnen voldoen aan de strengste normen voor privacy- en gegevensbescherming moeten zij echter dikwijls samenwerken met andere partijen uit de app-sector, zoals de fabrikanten van besturingssystemen en apparaten, app-winkels en derden, waaronder leveranciers van onderzoeksdiensten en advertentienetwerken.

App-ontwikkelaars moeten

- hun verplichtingen als voor de verwerking verantwoordelijke kennen en nakomen wanneer zij de gegevens van en over gebruikers verwerken;
- hun verplichtingen als voor de verwerking verantwoordelijke kennen en nakomen wanneer zij gegevensverwerkers inschakelen, bijvoorbeeld bij de uitbesteding van het verzamelen en verwerken van persoonsgegevens aan ontwikkelaars, programmeurs of aanbieders van online opslagvoorzieningen;
- om toestemming vragen voordat de app informatie op het apparaat verzamelt of plaatst, d.w.z. voordat de app wordt geïnstalleerd; bij deze toestemming moet het om een vrije, specifieke en op informatie berustende wilsuiting gaan;
- om gespecificeerde toestemming vragen voor elke soort gegevens waartoe de app toegang zoekt, en in ieder geval voor de categorieën locatie, contacten, unieke identificatiegegevens, identiteit van de betrokkene, identiteit van de telefoon, creditcard- en betalingsgegevens, telefonie en sms, browsergeschiedenis, e-mail, inloggegevens van sociale netwerken en biometrische gegevens;
- beseffen dat toestemming geen rechtvaardiging vormt voor excessieve of onevenredige gegevensverwerking;
- voorafgaand aan de installatie een duidelijke en begrijpelijke omschrijving bieden van de doeleinden van de gegevensverwerking en deze doeleinden niet veranderen zonder opnieuw om toestemming te vragen; volledige informatie bieden als de gegevens zullen worden gebruikt voor de doeleinden van derden, zoals reclame of onderzoeksdiensten;
- gebruikers de mogelijkheid bieden hun toestemming in te trekken en de app te de-installeren, en waar nodig de gegevens te wissen;
- het beginsel van gegevensminimalisering in acht nemen en alleen die gegevens verzamelen die strikt noodzakelijk zijn voor het gebruik van de gewenste functionaliteit;
- de noodzakelijke organisatorische en technische maatregelen treffen om bescherming te garanderen van de gegevens die zij verwerken, in alle ontwerp- en implementatiefasen van de app (ingebouwde privacybescherming), zoals bepaald in punt 3.6 van dit advies;
- de gebruikers van de app een duidelijk aanspreekpunt bieden;
- een leesbare, begrijpelijke en gemakkelijk toegankelijke uiteenzetting van het privacybeleid bieden, die gebruikers ten minste informeert over:
  - wie zij zijn (naam en contactgegevens);
  - de exacte categorieën persoonsgegevens die de app-ontwikkelaar zal verzamelen en verwerken;
  - waarom de gegevensverwerking noodzakelijk is (voor welke doeleinden);

- of er gegevens zullen worden doorgegeven aan derden (geen algemene, maar een specifieke beschrijving van degenen aan wie de gegevens eventueel zullen worden doorgegeven);
- welke rechten gebruikers hebben, zoals het intrekken van toestemming en het wissen van gegevens;

- app-gebruikers in staat stellen om hun recht op toegang, rectificatie en verwijdering van hun persoonsgegevens uit te oefenen en om bezwaar te maken tegen verwerking, en hen informeren over het bestaan van deze mogelijkheden;
- een redelijke bewaartermijn vaststellen voor gegevens die met de app zijn verzameld, alsook een periode van inactiviteit waarna de account als verlopen zal worden beschouwd;
- met betrekking tot apps die zijn bestemd voor kinderen, moeten zij: de leeftijdsgrens voor kinderen en minderjarigen in acht nemen, zoals vastgesteld in de nationale wetgeving; bij gegevensverwerking de meest restrictieve aanpak toepassen onder volledige inachtneming van de beginselen van minimale gegevensinzameling en de beperking van verwerkingsdoeleinden; zich onthouden van de verwerking van de gegevens van kinderen voor gedragsgerichte reclame, ongeacht of deze direct dan wel indirect is; zich ervan onthouden aan kinderen gegevens te vragen over hun familieleden en/of vrienden.

De werkgroep adviseert app-ontwikkelaars

- de toepasselijke richtsnoeren te bestuderen met betrekking tot de specifieke beveiligingsrisico's en -maatregelen;
- gebruikers proactief te informeren over inbreuken op persoonsgegevens overeenkomstig de vereisten van de e-privacyrichtlijn;
- gebruikers te informeren over de evenredigheidscriteria die zij hanteren voor de verschillende soorten gegevens die op het apparaat worden verzameld of geraadpleegd, alsook over de bewaartermijnen en de toegepaste beveiligingsmaatregelen;
- hulpmiddelen te ontwikkelen die gebruikers in staat stellen de bewaartermijnen voor hun persoonsgegevens aan te passen op grond van hun specifieke voorkeuren en omstandigheden, in plaats van hun van te voren vastgestelde bewaartermijnen te bieden;
- informatie in hun privacybeleid op te nemen voor Europese gebruikers;
- eenvoudige, maar veilige online toegangsinstrumenten voor gebruikers te ontwerpen en te implementeren, zonder dat dit leidt tot een verdere, overmatige verzameling van persoonsgegevens;
- hun creatieve talent, in samenwerking met de fabrikanten van besturingssystemen en app-winkels, te gebruiken om innovatieve oplossingen te ontwikkelen om gebruikers op gepaste wijze op hun mobiele apparaten te informeren, bijvoorbeeld door een systeem van getrapte meldingen gecombineerd met begrijpelijke iconen.

App-winkels moeten

- hun verplichtingen als voor de verwerking verantwoordelijke kennen en nakomen wanneer zij de gegevens van en over gebruikers verwerken;
- de informatieplicht van de app-ontwikkelaar handhaven, inclusief informatie over de soorten gegevens waartoe de app toegang kan krijgen en voor welke doeleinden, alsook of de gegevens worden gedeeld met derden;
- speciale aandacht besteden aan apps bestemd voor kinderen om hen te beschermen tegen de onrechtmatige verwerking van hun gegevens, en met name de nakoming garanderen van de verplichting om de relevante informatie op een eenvoudige manier weer te geven, rekening houdend met de leeftijd van de gebruiker;
- gedetailleerde informatie verstrekken over de toelatingscontroles voor apps die zij uitvoeren, ook wat de beoordeling van de privacy- en gegevensbescherming betreft.

De werkgroep adviseert app-winkels

- in samenwerking met de fabrikant van het besturingssysteem controle-instrumenten voor gebruikers te ontwikkelen, zoals symbolen die aangeven dat gegevens worden geraadpleegd of aangemaakt op het apparaat;
- alle apps te onderwerpen aan een openbaar beoordelingsmechanisme;

- een mechanisme in te voeren dat het mogelijk maakt om apps op een privacyvriendelijke manier op afstand te de-installeren;
- gebruikers feedbackkanalen te bieden om privacy- en/of beveiligingsproblemen te melden;
- samen te werken met app-ontwikkelaars om gebruikers op proactieve wijze te informeren over inbreuken op hun persoonsgegevens;
- app-ontwikkelaars te waarschuwen over de specifieke aspecten van de Europese wetgeving voordat zij de app in Europa op de markt brengen, bijvoorbeeld over het toestemmingsvereiste en de regels die van toepassing zijn wanneer persoonsgegevens worden overgedragen aan derde landen.

Fabrikanten van besturingssystemen en apparaten moeten

- hun API's, opslagnormen en gebruikersinterfaces bijwerken om gebruikers voldoende mogelijkheden te bieden om geldige toestemming te kunnen geven voor de verwerking van gegevens door apps;
- procedures voor het verkrijgen van toestemming inbouwen in hun besturingssysteem, welke geactiveerd worden wanneer de app voor het eerst wordt geopend of wanneer de app voor het eerst toegang probeert te krijgen tot een categorie gegevens die belangrijke gevolgen voor de privacy kan hebben;
- gebruikmaken van "ingebouwde privacy"-beginselen om te voorkomen dat de gebruiker heimelijk wordt gevolgd;
- de veiligheid van de verwerking garanderen;
- garanderen dat de (standaardinstellingen van) voorgeïnstalleerde apps voldoen aan de Europese wetgeving op het gebied van gegevensbescherming;
- gespecificeerde toegang bieden tot gegevens, sensoren en diensten om ervoor te zorgen dat de app-ontwikkelaar alleen toegang kan krijgen tot gegevens die noodzakelijk zijn voor de werking van de app;
- gebruiksvriendelijke, doeltreffende hulpmiddelen bieden om te voorkomen dat de gebruiker gevolgd wordt door adverteerders of andere derden, waarbij de standaardinstellingen gericht moeten zijn op het voorkomen van tracking;
- de beschikbaarheid garanderen van geschikte procedures om de eindgebruiker te informeren en voor te lichten over de mogelijkheden van apps en de gegevens waartoe zij toegang kunnen krijgen;
- ervoor zorgen dat de toegang tot iedere categorie gegevens wordt weergeven in de informatie aan de gebruiker voordat de app wordt geïnstalleerd, waarbij de weergegeven categorieën duidelijk en begrijpelijk moeten zijn;
- een omgeving creëren die bevorderlijk is voor de veiligheid, met inbegrip van hulpmiddelen die de verspreiding van schadelijke apps helpen voorkomen, en het mogelijk maken om iedere functionaliteit gemakkelijk te installeren/de-installeren.

De werkgroep adviseert de fabrikanten van besturingssystemen en apparaten

- gebruikers in staat te stellen apps te de-installeren en een signaal aan de app-ontwikkelaar te sturen (bijvoorbeeld via de API) om het wissen van de desbetreffende gebruikersgegevens mogelijk te maken;
- systematisch regelmatige beveiligingsupdates aan te bieden en beschikbaar te stellen;
- ervoor te zorgen dat de methoden en functies die toegang bieden tot persoonsgegevens de mogelijkheid bieden tot verwerking van verzoeken om gespecificeerde toestemming;
- actief iconen te helpen ontwikkelen en beschikbaar te stellen, die gebruikers wijzen op het gebruik van hun gegevens door apps;
- duidelijke logbestanden te ontwikkelen waarmee eindgebruikers een goed inzicht kunnen krijgen in de apps die toegang hebben verkregen tot de gegevens op hun apparaat en de hoeveelheid uitgaand verkeer per app in verhouding tot het door de gebruiker geïnitieerde verkeer.

Derden moeten

- hun verplichtingen als voor de verwerking verantwoordelijke kennen en nakomen wanneer zij gegevens (afkomstig) van gebruikers verwerken;

- voldoen aan het toestemmingsvereiste voorzien in artikel 5, lid 3, van de e-privacyrichtlijn wanneer zij gegevens op mobiele apparaten raadplegen of plaatsen, zulks in samenwerking met app-ontwikkelaars en/of app-winkels, welke in principe de gebruiker informatie bieden over de doeleinden van de gegevensverwerking;
- niet de mechanismen omzeilen die bedoeld zijn om tracking te voorkomen, zoals momenteel vaak gebeurd met de opties voor "Niet volgen" die in browsers zijn opgenomen;
- (voor leveranciers van communicatiediensten) wanneer zij apparaten onder eigen merk op de markt brengen, ervoor zorgen dat gebruikers geldige toestemming geven voor verwerking door voorgeïnstalleerde apps en hun verantwoordelijkheid nemen wanneer zij een bijdrage leveren aan de invulling van bepaalde eigenschappen van het apparaat en het besturingssysteem, bijvoorbeeld wanneer zij de toegang van de gebruiker tot bepaalde configuratie-instellingen beperken of de terbeschikkingstelling van herstelprogramma's filteren (voor beveiligings- of functionele problemen) die door de fabrikant van het apparaat of het besturingssysteem worden aangeboden;
- (voor adverteerders) zich er specifiek van onthouden buiten de app om reclame aan te bieden, zoals het aanbieden van advertenties door de browserinstellingen te wijzigen of iconen op het bureaublad van een mobiele telefoon te plaatsen, en zich onthouden van het gebruik van de unieke identificatiegegevens van een apparaat of een abonnee voor trackingdoeleinden;
- zich onthouden van de verwerking van de gegevens van kinderen ten behoeve van gedragsgerichte reclame, ongeacht of dit direct dan wel indirect is; dit omvat mede de veilige verzending en gecodeerde opslag van de unieke identificatiegegevens van het apparaat en de app-gebruiker, alsook van andere persoonsgegevens.

De werkgroep adviseert derden

- eenvoudige, maar veilige online toegangsinstrumenten voor gebruikers te ontwerpen en te implementeren, zonder dat dit leidt tot een verdere, overmatige verzameling van persoonsgegevens;
- alleen gegevens te verzamelen en te verwerken die logisch zijn gezien de context waarin de gebruiker de gegevens verstrekt.