GROEP GEGEVENSBESCHERMING ARTIKEL 29

1471/14/NL
WP 223

Advies 8/2014 over de recente ontwikkelingen op het gebied van het internet van de dingen

Uitgebracht op 16 september 2014

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien het bepaalde in artikel 29 en 30 van deze richtlijn,

Gezien het reglement van orde,

HEEFT HET ONDERHAVIGE ADVIES VASTGESTELD:

SAMENVATTING

Het internet van de dingen (Internet of Things, IoT) staat op het punt om een integraal onderdeel te worden van het leven van Europese burgers. Hoewel van menig project van het IoT de levensvatbaarheid nog niet vaststaat, worden er inmiddels "intelligente dingen" beschikbaar gemaakt die thuis, in de auto, op het werk of bij fysieke activiteiten metingen verrichten en communiceren. Nu al voorzien onlinetoestellen op de grootschalige markten voor zelfkwantificatie en domotica in de behoeften van EU-burgers. Het IoT biedt derhalve uitzicht op aanzienlijke groeimogelijkheden voor een groot aantal innoverende en creatieve bedrijven in de EU die – groot of klein – op deze markten opereren.

In het belang van zowel burgers als bedrijven in de EU zou de Groep artikel 29 graag zien dat aan deze verwachtingen wordt beantwoord. Bij het nastreven van de verwachte voordelen moet echter ook rekening worden gehouden met de vele uitdagingen die het IoT biedt voor de persoonlijke levenssfeer en de beveiliging. Er rijzen veel vragen over de kwetsbaarheid van deze apparaten, die dikwijls buiten een traditionele IT-infrastructuur worden gebruikt, zonder voldoende ingebouwde beveiliging. Gegevensverlies, besmetting door malware, maar ook ongeoorloofde toegang tot persoonsgegevens, inbreuk op de persoonlijke levenssfeer met wearables en onwettig toezicht zijn risico's die IoT-belanghebbenden moeten aanpakken om hun producten of diensten aantrekkelijk te maken voor toekomstige eindgebruikers.

Het gaat hierbij niet slechts om de naleving van technische en wettelijke normen, maar om de gevolgen van het IoT voor de samenleving als geheel. Organisaties die de bescherming van de persoonlijke levenssfeer en gegevens centraal stellen bij hun productontwikkeling, zullen in staat zijn om ervoor te zorgen dat hun producten in overeenstemming zijn met de beginselen van privacy-by-design en dat ze de privacyvriendelijke standaardinstellingen hebben waar de burgers van de EU op rekenen.

Tot nu toe is deze analyse slechts in zeer algemene bewoordingen onder de aandacht gebracht door een aantal regelgevers en belanghebbenden in de EU en elders. Om voortgang te boeken in deze kwestie heeft de Groep besloten dit advies uit te brengen. Zodoende tracht de Groep een bijdrage te leveren aan de eenvormige toepassing van het rechtskader voor gegevensbescherming op het IoT, alsmede aan de ontwikkeling van een hoog niveau van bescherming van persoonsgegevens in de EU. Naleving van dit kader is essentieel om het hoofd te bieden aan voornoemde wettelijke en technische uitdagingen, maar is ook van groot belang uit maatschappelijk oogpunt, aangezien gegevensbescherming als een fundamenteel mensenrecht geldt.

Derhalve worden in dit advies eerst de belangrijkste risico's voor de gegevensbescherming geïnventariseerd die inherent zijn aan het ecosysteem van het IoT. Vervolgens worden er richtlijnen gegeven voor de toepassing van het rechtskader van de EU in deze context. De Groep is er voorstander van dat belanghebbenden in hun projecten maximale garanties voor individuele gebruikers opnemen. Met name dienen gebruikers gedurende de hele productcyclus volledige controle te houden over hun persoonsgegevens; indien de verwerking door organisaties op basis van toestemming plaatsvindt, moet deze toestemming vrij, specifiek en geïnformeerd zijn. Met het oog daarop heeft de Groep uitvoerige aanbevelingen opgesteld voor de verschillende belanghebbenden (fabrikanten van apparaten, ontwikkelaars van toepassingen, sociale platforms, andere ontvangers van gegevens en normalisatie-instellingen) om hen te ondersteunen bij het voorzien in bescherming van gegevens en de persoonlijke levenssfeer bij hun producten en diensten.

De regie in handen geven van individuele personen door hen te informeren en hun vrijheid en veiligheid te waarborgen, is de sleutel tot vertrouwen en innovatie en daardoor tot succes op deze

markten. De Groep is ervan overtuigd dat belanghebbenden die aan deze verwachtingen beantwoorden, een zeer sterke concurrentiepositie zullen hebben tegenover spelers wier bedrijfsmodel erop gestoeld is om hun klanten niet te informeren over de mate waarin hun gegevens worden verwerkt en gedeeld en om hun klanten op te sluiten in hun ecosystemen.

Met het oog op de aanzienlijke uitdagingen op het gebied van gegevensbescherming in verband met het IoT zal WP29 de ontwikkelingen op dit gebied blijven volgen. De Groep blijft openstaan voor samenwerking op deze punten met nationale of internationale wetgevers en toezichthouders. Ook blijft de Groep bereid om te overleggen met vertegenwoordigers van het maatschappelijk middenveld en de sector, met name als deze belanghebbenden binnen de EU opereren als voor de verwerking verantwoordelijke of als gegevensverwerker.

INLEIDING

Het concept "internet van de dingen" (Internet of Things, IoT) heeft betrekking op een infrastructuur waarin miljarden sensoren zijn ingebouwd in alledaagse apparaten – "dingen" als zodanig, of dingen die gekoppeld zijn aan andere voorwerpen of aan individuen – voor de registratie, verwerking, opslag en doorgifte van gegevens; dankzij unieke identificatoren vindt via netwerken communicatie met andere apparaten of systemen plaats. Omdat het IoT gestoeld is op het principe van grootschalige gegevensverwerking via deze sensoren, die zijn ontworpen voor onmerkbare communicatie en naadloze gegevensuitwisseling, hangt het nauw samen met "pervasive computing" of "ubiquitous computing" (alomtegenwoordige gegevensverwerking).

Belanghebbenden bij het IoT stellen zich ten doel nieuwe toepassingen en diensten aan te bieden door het verzamelen en verder combineren van deze gegevens over individuen. Daarbij kan het "alleen maar" gaan om omgevingsspecifieke metingen ten aanzien van de gebruiker, maar ook om observatie en analyse van zijn gewoonten. Met andere woorden, het IoT brengt doorgaans de verwerking met zich mee van gegevens die betrekking hebben op geïdentificeerde of identificeerbare natuurlijke personen en die derhalve persoonsgegevens zijn in de zin van artikel 2 van de EU-richtlijn inzake gegevensbescherming.

De verwerking van dergelijke gegevens in deze context is afhankelijk van het gecoördineerde optreden van een aanzienlijk aantal belanghebbenden (al dan niet als gegevensplatform optredende fabrikanten van apparaten, gegevensverzamelaars en gegevensmakelaars, ontwikkelaars van toepassingen, sociale platforms, (ver)huurders van apparaten enz.). Hun respectieve rollen worden verderop in dit advies besproken. Deze verschillende belanghebbenden kunnen om diverse redenen betrokken zijn, bijvoorbeeld om te voorzien in aanvullende functies of gebruiksvriendelijke bedieningsinterfaces voor het beheer van technische en privacygerelateerde instellingen, of omdat gebruikers doorgaans toegang tot hun verzamelde gegevens hebben via een aparte webgebaseerde interface. Bovendien kunnen gegevens, indien ze eenmaal op afstand zijn opgeslagen, met andere partijen worden gedeeld, soms zonder dat de betrokkene zich hiervan bewust is[1]. In deze gevallen wordt de verdere doorgifte van de persoonsgegevens opgelegd aan de gebruiker, die dit niet kan voorkomen zonder de meeste functies van het apparaat uit te schakelen. Het resultaat van deze keten van handelingen is dat het IoT de fabrikanten van apparaten en hun handelspartners in staat stelt te beschikken over zeer gedetailleerde gebruikersprofielen of deze aan te leggen.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

Uit het bovenstaande blijkt dat de ontwikkeling van het IoT aanzienlijke nieuwe uitdagingen oplevert op het gebied van de bescherming van persoonsgegevens en de persoonlijke levenssfeer[2]. Indien aan bepaalde ontwikkelingen van het IoT niet de hand wordt gehouden, kunnen zij zelfs tot vormen van toezicht op personen leiden die die wellicht niet in overeenstemming zijn met de EU-wetgeving. Ook zijn er aanmerkelijke zorgen over de beveiliging van het IoT, omdat inbreuken op de beveiligingsvoorschriften aanzienlijke risico's voor de persoonlijke levenssfeer met zich kunnen meebrengen voor de personen om wier verwerkte gegevens het gaat.

De Groep heeft derhalve besloten het onderhavige advies uit te brengen om een bijdrage te leveren aan de vaststelling van en het toezicht op de risico's die voortvloeien uit deze activiteiten en die raken aan de grondrechten van burgers van de EU.

[2] Dit advies dient ook te worden gelezen in samenhang met de adviezen die de Groep in 2014 heeft uitgebracht over de toepassing van de begrippen noodzakelijkheid en evenredigheid en over gegevensbescherming in de rechtshandhavingssector (WP211) en over bewaking van elektronische communicatie (WP 215).

1. Reikwijdte van het advies: bijzondere aandacht voor drie ontwikkelingen op het gebied van het IoT

In dit stadium is het onmogelijk om te voorspellen in welke mate het IoT tot ontwikkeling zal komen. Deels komt dit doordat nog grotendeels onduidelijk is hoe alle gegevens die via het IoT kunnen worden verzameld, een nuttige en commercieel haalbare toepassing kunnen vinden. Eveneens is onduidelijk of het IoT kan leiden tot synergieën en convergentie met andere technologische ontwikkelingen als cloud computing en voorspellende analyses, omdat het vooralsnog prille marktontwikkelingen betreft.

De Groep heeft daarom besloten om dit advies voornamelijk toe te spitsen op drie specifieke ontwikkelingen op het gebied van het IoT ("wearable computing", zelfkwantificatie en domotica), die 1) gepaard gaan met een rechtstreekse gebruikersinterface en 2) betrekking hebben op apparaten en diensten waarvan daadwerkelijk gebruik wordt gemaakt, zodat ze kunnen worden geanalyseerd in het licht van de wetgeving inzake gegevensbescherming. Dit advies gaat daarom niet specifiek in op B2B-toepassingen en ontwikkelingen als "intelligente steden", "intelligente vervoermiddelen" en ontwikkelingen op het gebied van M2M ("machine to machine"). De beginselen en aanbevelingen in dit advies kunnen echter ook buiten het precieze toepassingsgebied ervan relevant zijn en betrekking hebben op andere ontwikkelingen betreffende het IoT.

1.1 **Wearable computing**

Onder wearable computing wordt het gebruik verstaan van alledaagse voorwerpen, zoals horloges, brillen en kleding, waarin sensoren zijn ingebouwd om hun functionaliteit uit te breiden. Omdat het hierbij gaat om vertrouwde alledaagse voorwerpen met een vergrote bruikbaarheid, zullen deze producten waarschijnlijk snel ingeburgerd raken, te meer omdat ze nauwelijks te onderscheiden zijn van vergelijkbare producten zónder online toepassing. Er kunnen camera's, microfoons en sensoren in ingebouwd zijn die gegevens kunnen registreren en doorgeven aan de fabrikant. Verder stimuleert de beschikbaarheid van een API voor wearables (bv. Adroid Wear[3]) de ontwikkeling van toepassingen door derde partijen, die zodoende toegang kunnen krijgen tot de gegevens die door deze dingen worden verzameld.

1.2 **Zelfkwantificatie**

Dingen die zelfkwantificatie mogelijk maken, zijn ontworpen om regelmatig te worden gedragen door personen die informatie over hun eigen gewoonten en leefwijze willen registreren. Zo kan iemand bijvoorbeeld iedere nacht een slaapmeter dragen om een uitgebreid beeld te krijgen van zijn slaappatronen. Andere apparaten zijn bedoeld voor het bijhouden van bewegingen, zoals activiteitenmeters voor een continue meting en registratie van kwantitatieve indicatoren die te maken hebben met de fysieke handelingen van een persoon, zoals aantallen verbrande calorieën of gelopen afstanden.

Sommige voorwerpen meten ook gewicht, polsslag en andere gezondheidsindicatoren. De verzamelde gegevens kunnen worden geanalyseerd om vast te stellen welke tendensen en veranderingen het gedrag in de loop van de tijd vertoont en kwalitatieve informatie over de gezondheid te verkrijgen. Zo kunnen tot op zekere hoogte bijvoorbeeld de kwaliteit en effecten van fysieke activiteit worden beoordeeld op basis van vooraf bepaalde drempelwaarden en de kans dat zich ziekteverschijnselen voordoen.

[3] http://developer.android.com/wear/index.html.

De sensoren voor zelfkwantificatie moeten vaak onder bepaalde omstandigheden worden gedragen om relevante informatie te extraheren. Zo kan een versnellingsmeter die aan de riem van een betrokkene wordt geplaatst, met geschikte algoritmen de bewegingen van de onderbuik meten *(ruwe gegevens)*, hieruit informatie extraheren over het ademhalingsritme *(geaggregeerde en geëxtraheerde gegevens)* en het stressniveau van de betrokkene weergeven *(toonbare gegevens)*. Bij sommige apparaten wordt alleen deze laatste informatie aan de gebruiker gemeld, maar hebben de fabrikant of dienstverlener mogelijk toegang tot veel meer gegevens, die in een later stadium kunnen worden geanalyseerd.

Zelfkwantificatie brengt uitdagingen met zich mee ten aanzien van het verzamelen van gegevenscategorieën die gezondheidsgerelateerd zijn, alsook ten aanzien van de grootschaligheid van deze verzameling. Omdat zelfkwantificatie erop gericht is gebruikers aan te sporen om gezond te blijven, zijn er vele verbanden met het ecosysteem van de e-gezondheid. De werkelijke nauwkeurigheid van de metingen en de daaraan verbonden conclusies is echter door recente onderzoeken in twijfel getrokken[4].

1.3 **Huisautomatisering ("domotica")**

Tegenwoordig kunnen IoT-apparaten ook in kantoren of huizen worden geplaatst, zoals onlineledlampen, thermostaten, rookalarmen, weerstations, wasmachines of ovens die via het internet op afstand kunnen worden bediend. Zo kunnen dingen met bewegingssensoren waarnemen en registreren wanneer een gebruiker thuis is en wat diens bewegingspatronen zijn en kunnen ze wellicht vooraf vastgestelde handelingen verrichten (bv. een lamp inschakelen of de kamertemperatuur veranderen). De meeste apparaten voor huisautomatisering zijn voortdurend online en kunnen gegevens terugsturen naar de fabrikant.

Uiteraard brengen domotica specifieke uitdagingen mee voor de bescherming van gegevens en de persoonlijke levenssfeer, aangezien een analyse van de gebruikspatronen waarschijnlijk details over leefwijze, gewoonten en keuzen oplevert of eenvoudig zal onthullen wanneer de bewoners thuis zijn.

De drie bovengenoemde categorieën apparaten zijn exemplarisch voor de belangrijkste vraagstukken in verband met de persoonlijke levenssfeer en het IoT in zijn huidige staat. Opgemerkt dient echter te worden dat deze categorieën elkaar niet uitsluiten: een wearable zoals een smartwatch kan worden gebruikt voor het bijhouden van de hartslag, d.w.z. voor zelfkwantificatie.

2. Uitdagingen voor de bescherming van gegevens en de persoonlijke levenssfeer in verband met het internet van de dingen

De Groep heeft besloten dit advies uit te brengen omdat het IoT een aantal aanzienlijke uitdagingen voor de bescherming van gegevens en de persoonlijke levenssfeer met zich meebrengt. Sommige uitdagingen zijn nieuw; andere bestaan al langer, maar worden nu groter door de exponentiële toename van de gegevensverwerking die met de ontwikkeling van het IoT gepaard gaat. Het belang van de toepassing van het EU-rechtskader voor gegevensbescherming en de overeenkomstige praktische aanbevelingen die hieronder volgen, moet in het licht van deze uitdagingen worden beschouwd.

2.1 **Gebrek aan controle en asymmetrische informatievoorziening**

Omdat pervasieve diensten op onmerkbare wijze moeten worden geleverd, is het mogelijk dat de gegevens van gebruikers in de praktijk door een derde partij zullen worden bijgehouden. Dit kan leiden tot situaties waarin de gebruiker de controle over de verspreiding van zijn gegevens volledig verliest, afhankelijk van de mate van transparantie waarin gegevens worden verzameld en verwerkt.

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results.

Meer in het algemeen levert alle interactie tussen voorwerpen, tussen voorwerpen en apparaten van personen, tussen personen en andere voorwerpen en tussen voorwerpen en backend-systemen gegevensstromen op die nauwelijks kunnen worden beheerd met de traditionele hulpmiddelen voor het verzekeren van een adequate bescherming van de rechten en belangen van de betrokkenen. Zo kunnen gegevens van het IoT in tegenstelling tot andere soorten content voorafgaand aan publicatie niet adequaat door de betrokkene worden gecontroleerd, hetgeen onmiskenbaar het risico meebrengt dat de gebruiker te weinig controle kan uitoefenen en buitensporig wordt blootgesteld. Ook kan communicatie tussen voorwerpen zowel automatisch als door middel van een standaardinstelling worden gestart, zonder dat de persoon zich hiervan bewust is. Zonder mogelijkheid om de interactie tussen dingen doeltreffend te beheersen of virtuele grenzen vast te stellen door voor bepaalde dingen werkzame en niet-werkzame zones te definiëren, wordt het bijzonder moeilijk om de gegenereerde gegevensstroom te beheersen. Nog moeilijker zal het zijn om het daaropvolgende gebruik te beheersen en doelverschuiving ("function creep") te voorkomen. Dit gebrek aan controle, waarvan ook sprake is bij andere technische ontwikkelingen zoals cloud computing en big data, is des te pregnanter omdat deze verschillende nieuwe technologieën ook nog kunnen worden gecombineerd.

2.2 **Kwaliteit van de toestemming van de gebruiker**

In veel gevallen is de gebruiker zich wellicht niet bewust van de gegevensverwerking die door bepaalde voorwerpen wordt verricht. Indien er sprake is van een dergelijk gebrek aan informatie, is het moeilijk aan te tonen dat de toestemming volgens het EU-recht geldig is, omdat de betrokkene daarvoor geïnformeerd dient te zijn. In voorkomend geval kan toestemming niet dienen als wettelijke grond voor gegevensverwerking uit hoofde van het EU-recht.

Wearables zoals smartwatches zijn ook niet opvallend[5]: voor de meeste mensen is een normaal horloge wellicht niet te onderscheiden van een smartwatch, terwijl deze laatste toch ingebouwde camera's, microfoons en bewegingssensoren bevat die gegevens kunnen registreren en doorgeven zonder dat de gebruiker zich daarvan bewust is – laat staan dat hij hiervoor toestemming heeft gegeven. Dit roept de vraag op hoe de gegevensverwerking waarbij wearables een rol spelen, vastgesteld kan worden. Een mogelijke oplossing is een geschikte markering die voor de betrokkenen zichtbaar zou zijn.

Bovendien is de mogelijkheid om af te zien van het gebruik van bepaalde diensten of functies van een IoT-apparaat zeker in bepaalde gevallen meer een theoretisch concept dan een reële optie. Dit roept de vraag op of de toestemming van de gebruiker met de onderliggende gegevensverwerking wel als vrij kan worden beschouwd en derhalve als geldig volgens het EU-recht.

Verder is het mogelijk dat traditionele mechanismen die worden aangewend om de toestemming van personen te verkrijgen, in het IoT moeilijk zijn toe te passen, hetgeen resulteert in toestemming "van slechte kwaliteit" vanwege een gebrek aan informatie of vanwege de feitelijke onmogelijkheid om toestemming zo te formuleren dat de betrokkene zijn voorkeuren precies te kennen geeft. In de praktijk lijkt het er op dat sensorapparaten doorgaans niet worden ontworpen om zelf informatie te geven, noch om een geldig mechanisme te bieden voor het verkrijgen van toestemming van de persoon. Belanghebbenden op het gebied van het IoT dienen evenwel nieuwe manieren te overwegen om de geldige toestemming van de gebruiker te verkrijgen, waaronder de implementatie van

[5] Zoals beschreven in Advies 02/2013 betreffende apps op intelligente apparaten brengen wearables belangrijke uitdagingen met zich mee vanwege de voortdurende verzameling van gegevens van anderen in de nabijheid en gedurende langere tijdsperiodes.

toestemmingsmechanismen via de apparaten zelf. Specifieke voorbeelden als "Privacy Proxies" en "Sticky Policies" komen later in dit document aan de orde.

2.3 Gevolgtrekkingen uit gegevens en aanpassing van het doel van oorspronkelijke verwerkingen

De toename van de hoeveelheid door het IoT gegenereerde gegevens maakt, in combinatie met moderne technieken voor analyse en onderlinge vergelijking van gegevens, deze gegevens wellicht zeer geschikt voor secundair gebruik, ongeacht of dit gebruik overeenstemt met de doelen van de oorspronkelijke verwerking. Derde partijen die toegang vragen tot gegevens die door andere partijen zijn verzameld, willen deze gegevens mogelijk voor geheel andere doeleinden gebruiken.

Schijnbaar onbelangrijke gegevens die oorspronkelijk via een apparaat zijn verzameld (bv. de versnellingsmeter en gyroscoop van een smartphone) kunnen vervolgens worden gebruikt om er andere informatie uit af te leiden met een geheel andere betekenis (bv. het rijgedrag van de persoon). Deze mogelijkheid om gevolgtrekkingen te baseren op zulke "ruwe" gegevens komt bovenop de traditionele risico's van sensorfusie, een in de computerwetenschap zeer bekend fenomeen[6].

Zelfkwantificatie illustreert ook hoeveel informatie kan worden afgeleid uit bewegingssensoren door middel van aggregatie en geavanceerde analyse. Bij deze apparaten wordt veelal gebruikgemaakt van elementaire sensoren om ruwe gegevens te registreren (bv. bewegingen van de betrokkene) en van geavanceerde algoritmen om waarneembare informatie te extraheren (bv. het aantal stappen) en hieruit mogelijk gevoelige informatie af te leiden die aan de eindgebruikers wordt getoond (bv. de fysieke conditie van de betrokkene).

Er zijn specifieke uitdagingen verbonden aan een dergelijke tendens. Hoewel de gebruiker geen bezwaar had tegen het delen van de oorspronkelijke informatie voor een bepaald doel, wenst hij misschien niet de secundaire informatie te delen die voor geheel andere doeleinden kan worden gebruikt. Daarom is het van belang dat belanghebbenden in het IoT er voor zorgen dat de gegevens op ieder niveau (ruwe, geëxtraheerde en weergegeven gegevens) alleen worden gebruikt voor doeleinden die in overeenstemming zijn met het oorspronkelijke doel van de verwerking en dat deze doeleinden bekend zijn bij de gebruiker.

2.4 In de persoonlijke levenssfeer doordringende herkenning van gedragspatronen en profilering

Hoewel afzonderlijke voorwerpen geïsoleerde gegevens zullen verzamelen, kunnen door het verzamelen en analyseren van voldoende gegevens bepaalde aspecten van de gewoonten, gedragingen en voorkeuren van personen worden blootgelegd. Zoals eerder beschreven zal het genereren van kennis uit triviale of zelfs anonieme gegevens door het snel toenemende aantal sensoren eenvoudig worden en een aanzienlijke mate van profilering mogelijk maken.

Door de analyse van informatie die is geregistreerd in een IoT-omgeving kunnen nog gedetailleerder en vollediger leef- en gedragspatronen worden ontwaard.

Deze tendens zal waarschijnlijk zelfs invloed hebben op de manier waarop de gebruiker zich gedraagt, zoals het wijdverbreide gebruik van CCTV het gedrag van burgers in openbare ruimten aantoonbaar heeft beïnvloed. Door het IoT kan dit soort potentiële toezicht doordringen tot de meest persoonlijke

[6] Bij sensorfusie worden sensorgegevens of aan andere bronnen ontleende gegevens gecombineerd om betere en nauwkeuriger informatie te verkrijgen dan mogelijk zou zijn met afzonderlijke bronnen.

levenssfeer van gebruikers, waaronder de huiselijke sfeer. Hierdoor komt de persoon onder druk te staan om ongebruikelijk gedrag te vermijden, teneinde te voorkomen dat "afwijkende" gedragingen worden opgemerkt. Een dergelijk tendens zou een grove inbreuk betekenen op het privéleven en de intimiteit van individuen en dient op de voet te worden gevolgd.

2.5 **Beperkte mogelijkheid tot anoniem gebruik van diensten**

De volledige ontwikkeling van de mogelijkheden van het IoT kan de huidige mogelijkheden om anoniem gebruik te maken van diensten en om in zijn algemeenheid onopgemerkt te blijven, onder druk zetten.

Zo kan de aanwezigheid van wearables in de nabijheid van betrokkenen andere identificatoren beschikbaar maken, zoals de MAC-adressen van andere apparaten die kunnen worden gebruikt om een vingerafdruk te maken voor het bijhouden van de locatie van de betrokkene. Het verzamelen van de MAC-adressen van meerdere sensorapparaten draagt bij tot het genereren van unieke vingerafdrukken en stabiele identificatoren die belanghebbenden op het gebied van het IoT in verband zullen kunnen brengen met specifieke personen. Deze vingerafdrukken en identificatoren kunnen worden gebruikt voor allerlei doeleinden, waaronder locatieanalyse[7] of de analyse van bewegingspatronen van menigtes en personen.

Bij een dergelijke tendens dient men in gedachten te houden dat zulke gegevens later kunnen worden gecombineerd met andere gegevens die van andere systemen afkomstig zijn (bv. CCTV of logbestanden van internet).

In zulke omstandigheden zijn sommige sensorgegevens bijzonder kwetsbaar voor heridentificatie-aanvallen.

In het licht van het bovenstaande is het duidelijk dat het steeds moeilijker zal worden om anoniem te blijven en de persoonlijke levenssfeer in stand te houden op het IoT. De ontwikkeling van het IoT brengt wat dat betreft aanzienlijke zorgen met zich mee ten aanzien van de bescherming van gegevens en de persoonlijke levenssfeer.

2.6 **Veiligheidsrisico's: veiligheid vs. efficiëntie**

Het IoT houdt een aantal uitdagingen in voor de veiligheid, met name doordat vereisten inzake beveiliging en hulpbronnen fabrikanten ertoe dwingen om een evenwicht te zoeken tussen batterijrendement en apparaatbeveiliging. In het bijzonder is nog onduidelijk welke balans fabrikanten van apparaten zullen vinden tussen enerzijds maatregelen voor vertrouwelijkheid, integriteit en beschikbaarheid op alle niveaus van het verwerkingsproces en anderzijds de noodzaak om het gebruik van computercapaciteit – en energie – door objecten en sensoren te optimaliseren.

Er bestaat dus een risico dat het IoT alledaagse objecten kan veranderen in mogelijke doelwitten voor inbreuken op de persoonlijke levenssfeer en de informatieveiligheid, terwijl het tegelijk zorgt voor een aanzienlijk wijdere verbreiding van deze doelwitten dan de huidige vorm van internet. Minder veilige onlineapparaten kunnen nieuwe doelwitten voor efficiënte aanvallen zijn. Hierbij valt te denken aan het gemak waarmee iets of iemand kan worden gevolgd en aan gegevensinbreuken waarbij persoonsgegevens worden gestolen of gecompromitteerd, met alle gevolgen van dien voor consumentenrechten en de perceptie van de veiligheid van het IoT.

[7] Locatieanalyse verwijst naar de analyse van het aantal mensen op een bepaalde plaats op een bepaalde tijd en de duur van hun aanwezigheid.

IoT-apparaten en -platformen zullen naar verwachting ook gegevens uitwisselen en opslaan op de infrastructuren van dienstverleners. Derhalve dient voor de veiligheid van het IoT niet alleen de beveiliging van apparaten in overweging te worden genomen, maar moet ook rekening worden gehouden met de communicatieverbindingen, de infrastructuur voor de opslag en andere inputs van dit ecosysteem.

Doordat er sprake is van verschillende verwerkingsniveaus, waarvan het technische ontwerp en de implementatie door verschillende belanghebbenden worden verzorgd, vindt er voldoende onderlinge coördinatie plaats en ontstaan er zwakke punten die kunnen worden uitgebuit.

Zo kunnen de meeste sensoren die momenteel op de markt zijn, geen versleutelde communicatieverbinding leggen, omdat de benodigde rekenkracht moeilijk kan worden opgebracht door een apparaat dat in zijn stroomvoorziening is beperkt door batterijen met een laag vermogen. Wat betreft end-to-end-beveiliging is bij de integratie van fysieke en logische onderdelen waarin door verschillende belanghebbenden wordt voorzien, de beveiliging maar zo sterk als het zwakste onderdeel.

3. Toepassing van de EU-wetgeving op de verwerking van persoonsgegevens in het IoT

3.1 **Toepasselijk recht**

Het EU-rechtskader voor de beoordeling van kwesties rond de bescherming van gegevens en de persoonlijke levenssfeer in verband met het IoT, bestaat uit Richtlijn 95/46/EG en specifieke bepalingen van Richtlijn 2002/58/EG, gewijzigd bij Richtlijn 2009/136/EG.

Dit kader is van toepassing indien wordt voldaan aan de voorwaarden van artikel 4 van Richtlijn 95/46/EG. De Groep heeft uitvoerige richtsnoeren gegeven omtrent de interpretatie van artikel 4, en wel in Advies 8/2010[8] over toepasselijk recht.

Volgens artikel 4, lid 1, onder a), van de richtlijn 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 partij op het grondgebied van de betreffende lidstaat. Dit begrip van vestiging in de context van de internetgebaseerde economie is onlangs zeer breed geïnterpreteerd door het Europese Hof van Justitie[9].

Het nationale recht van een lidstaat is ook van toepassing indien de voor de verwerking verantwoordelijke persoon niet gevestigd is op het grondgebied van de Gemeenschap, maar voor de verwerking van persoonsgegevens gebruikmaakt van „middelen" die zich op het grondgebied van genoemde lidstaat bevinden (artikel 4, lid 1, onder c)). Een belanghebbende bij het IoT die krachtens Richtlijn 95/46/EG wordt aangemerkt als voor de verwerking verantwoordelijke en die niet in de EU is gevestigd in de zin van artikel 4, lid 1, onder a) (en betrokken is bij de ontwikkeling, distributie of exploitatie van IoT-apparaten), zal derhalve waarschijnlijk onderhevig zijn aan EU-wetgeving, voor zover de belanghebbende gegevens verwerkt via de „middelen" van gebruikers in de EU.

Alle voorwerpen die worden gebruikt om de gegevens van de persoon te verzamelen en verder te verwerken in het kader van de dienstverlening via het IoT worden aangemerkt als middelen in de zin van de richtlijn. Deze kwalificatie is uiteraard van toepassing op de apparaten zelf (stappentellers, slaapmeters, onlinehuisapparatuur zoals thermostaten, rookmelders, onlinebrillen of -horloges, enz.).

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_nl.pdf.
[9] Arrest van het Hof (Grote kamer), van 13 mei 2014, in zaak C-131/12 (punten 45 tot en met 60).

Ze is ook van toepassing op de eindapparaten (bv. smartphones of tablets) waarop vooraf software of apps zijn geïnstalleerd om zowel de omgeving van de gebruiker te meten door middel van ingebouwde sensoren of netwerkinterfaces als de gegevens vervolgens door deze apparaten te laten versturen naar de verschillende voor de verwerking verantwoordelijke partijen.

Het vaststellen van de rol van de verschillende belanghebbenden bij het IoT is essentieel voor de kwalificatie van hun wettelijke status als voor de verwerking verantwoordelijken en derhalve voor de vaststelling van de nationale wet die op de door hen geïmplementeerde verwerking van toepassing is, alsook hun respectieve verantwoordelijkheden. De vaststelling van de rol van de bij het IoT betrokken partijen zal onder punt 3.3 worden geanalyseerd.

3.2 **Het begrip persoonsgegevens**

De EU-wetgeving is van toepassing op de verwerking van persoonsgegevens zoals gedefinieerd in artikel 2 van Richtlijn 95/46/EG. De Groep heeft uitvoerige richtsnoeren gegeven omtrent de interpretatie van dit begrip, en wel in Advies 4/2007[10] over het begrip persoonsgegeven.

In de context van het IoT kan een persoon vaak worden geïdentificeerd op basis van gegevens die van "dingen" afkomstig zijn. Met zulke gegevens is het zelfs mogelijk het leefpatroon van een bepaald persoon of gezin te ontwaren – bv. gegevens gegenereerd door centrale bediening van de verlichting, verwarming, ventilatie en airconditioning.

Bovendien dienen zelfs pas na pseudonimisering of zelfs anonimisering te verwerken gegevens over personen wellicht ook als persoonsgegevens te worden beschouwd. De grote hoeveelheid automatisch verwerkte gegevens in het IoT brengt risico's van heridentificatie met zich mee. Wat dit betreft verwijst de Groep naar de relevante ontwikkelingen beschreven in het recente advies over anonimiseringstechnieken, waarin een bijdrage aan de vaststelling van deze risico's wordt geleverd en aanbevelingen worden gedaan ten aanzien van de implementatie van deze technieken[11].

3.3 **Belanghebbenden bij het IoT als verantwoordelijken voor gegevensverwerking in de EU**

De verhouding tussen de begrippen "voor de verwerking verantwoordelijke" en "verwerker" staat centraal bij de toepassing van Richtlijn 95/46/EG. De respectieve verantwoordelijkheden van de verschillende organisaties die bij gegevensverwerking betrokken zijn, worden namelijk door deze begrippen bepaald. Belanghebbenden kunnen teruggrijpen op Advies 1/2010, waarin de Groep richtsnoeren biedt voor de toepassing van de begrippen "voor de verwerking verantwoordelijke" en "verwerker"[12] als het gaat om complexe systemen met meerdere partijen. Daarbij is in vele scenario's sprake van voor de verwerking verantwoordelijken en verwerkers, zelfstandig of gezamenlijk, met verschillende maten van autonomie en verantwoordelijkheid.

De implementatie van het IoT brengt doorgaans het gecombineerde optreden met zich mee van een aanzienlijk aantal belanghebbenden, zoals fabrikanten van apparaten, sociale platforms, toepassingen van derde partijen, (ver)huurders van apparaten, gegevensmakelaars[13] of gegevensplatforms.

---

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[11] Advies 05/2014 over anonimiseringstechnieken, vastgesteld op 10 april 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf.

[12] Advies 01/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", vastgesteld op 16 februari 2010 (WP 169), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf

[13] Gegevensmakelaars kopen gegevens bij bedrijven in om lijsten op te stellen van personen die tot een categorie of groep behoren. Deze categorieën en groepen worden door de gegevensmakelaars opgesteld en kunnen een

Het complexe web van betrokken belanghebbenden maakt het noodzakelijk om wettelijke verantwoordelijkheden met betrekking tot de verwerking van de persoonsgegevens zorgvuldig aan hen toe te wijzen op basis van het specifieke karakter van hun optreden.

3.3.1 Fabrikanten van apparaten

Fabrikanten van apparaten in het IoT beperken zich niet tot de verkoop van fysieke artikelen aan hun klanten of het leveren van merkloze producten aan andere organisaties. Het kan ook zijn dat ze het besturingssysteem van het ding hebben ontwikkeld of aangepast of software hebben geïnstalleerd die bepalend is voor de algehele functionaliteit ervan, waaronder de verzameling van gegevens en de frequentie hiervan, en wanneer gegevens aan wie worden doorgegeven en voor welke doeleinden (bedrijven zouden bijvoorbeeld de verzekeringspremies van hun werknemers kunnen vaststellen op basis van gegevens gemeld door meetapparaten die ze hen laten dragen[14]). De meeste fabrikanten verzamelen en verwerken door het apparaat gegenereerde persoonsgegevens voor doeleinden en op wijzen die geheel door hen zijn bepaald. Derhalve moeten zij krachtens de EU-wetgeving worden aangemerkt als voor verwerking verantwoordelijken.

3.3.2 Sociale platforms

Als betrokkenen gegevens van onlinedingen in het openbaar of met andere gebruikers kunnen delen, is het nog waarschijnlijker dat ze deze dingen gaan gebruiken. Met name gebruikers van apparaten voor zelfkwantificatie zijn geneigd gegevens op sociale netwerken met anderen te delen om een vorm van positieve wedijver binnen de groep te stimuleren.

Een dergelijk delen op sociale netwerken van door "dingen" verzamelde en geaggregeerde gegevens vindt vaak automatisch plaats indien de toepassing eenmaal door de gebruiker zo is ingesteld. Bij levering door de fabrikant behoort de mogelijkheid om te delen doorgaans tot de standaardinstellingen van toepassingen.

Dat deze meldingen op sociale platforms geaggregeerd worden, betekent dat er nu specifieke verantwoordelijkheden voor gegevensbescherming bij deze platforms komen te liggen. Als sociale netwerken deze gegevens, die zij van de gebruikers ontvangen, verwerken voor aparte door henzelf bepaalde doeleinden, moeten zij krachtens de EU-wetgeving worden aangemerkt als voor de gegevensverwerking verantwoordelijken. Zo kan een sociaal netwerk uit door een stappenteller verzamelde gegevens afleiden dat een gebruiker regelmatig hardloopt en deze persoon op basis hiervan reclame over hardloopschoenen tonen. De gevolgen hiervan zijn nader uiteengezet in het eerdere Advies over online sociale netwerken[15] van WP29.

3.3.3 Ontwikkelaars van toepassingen als derde partij

Veel sensoren werken met API's om de ontwikkeling van toepassingen te vergemakkelijken. Om deze toepassingen te gebruiken moeten betrokkenen toepassingen van derde partijen installeren die hen in staat stellen toegang te krijgen tot hun gegevens die zijn opgeslagen door de fabrikant. De installatie van deze toepassingen houdt vaak in dat de ontwikkelaar van de toepassingen via de API toegang wordt geboden tot de gegevens.

---

weerspiegeling vormen van demografische kenmerken, inkomens of getoonde belangstelling voor een bepaald onderwerp of product.

[14] Met volgapparatuur zouden werkgevers de gezondheid van werknemers in het oog kunnen houden, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health.

[15] Advies 5/2009 over online sociale netwerken, goedgekeurd op juni 12 2009 (WP 163) - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_nl.pdf

Sommige toepassingen belonen gebruikers voor specifieke dingen. Zo zou een zorgverzekeraar gebruikers kunnen belonen voor het gebruiken van apparaten voor zelfkwantificatie of zou een woonhuisverzekeraar een specifieke toepassing kunnen ontwikkelen om ervoor te zorgen dat de onlinebrandmelders van hun klanten correct ingesteld zijn. Tenzij deze gegevens goed geanonimiseerd worden, wordt een dergelijke toegang op grond van artikel 2 van Richtlijn 95/46/EG aangemerkt als een verwerking. Dit betekent dat de ontwikkelaar van de toepassing die deze gegevens heeft georganiseerd, volgens EU-wetgeving dient te worden beschouwd als voor de verwerking verantwoordelijke.

Dergelijke toepassingen worden traditioneel geïnstalleerd op basis van een opt-in. Gezien het feit dat voor een dergelijke toegang voorafgaande toestemming van de gebruiker is vereist, dient deze toestemming vrij en specifiek te zijn en op informatie te berusten. In de praktijk blijkt echter dat als ontwikkelaars van toepassingen als derde partij om toestemming verzoeken , niet voldoende informatie wordt weergegeven om de toestemming van de gebruiker te kunnen beschouwen als specifiek en op voldoende informatie berustend en derhalve als geldig volgens de EU-wetgeving.

3.3.4 Andere derde partijen

Naast fabrikanten van apparaten en ontwikkelaars van toepassingen zijn er meer derde partijen die apparaten voor het IoT kunnen gebruiken voor de verzameling en verwerking van informatie over personen. Het zou bijvoorbeeld kunnen dat zorgverzekeraars stappentellers aan klanten willen geven om te meten hoe vaak zij aan lichaamsbeweging doen[16] en hun premies hieraan aan te passen.

In tegenstelling tot fabrikanten van apparaten hebben zulke derde partijen geen controle over het type gegevens dat door het ding wordt verzameld. Ze worden echter wel aangemerkt als voor verwerking verantwoordelijk omdat zij de door zulke IoT-apparaten gegenereerde gegevens verzamelen en bewaren voor specifieke door henzelf bepaalde doeleinden.

Voorbeeld: een verzekeringsbedrijf start een campagne en biedt een stappenteller aan voor leden die in aanmerking willen komen voor lagere tarieven. Leden die op het aanbod ingaan, ontvangen een door het bedrijf ingestelde en geregistreerde stappenteller. Terwijl de abonnees toegang hebben tot de door hun stappenteller geregistreerde gegevens, zijn de apparaten zelf eigendom van "FeelGood", dat ook toegang heeft tot de gegevens van zijn abonnees. In dit kader dienen abonnees te worden beschouwd als betrokkenen en toegang te krijgen tot hun account op de toepassing voor de stappenteller, terwijl het verzekeringsbedrijf wordt aangemerkt als voor de verwerking verantwoordelijke.

3.3.5 IoT-gegevensplatforms

Vanwege een gebrek aan standaardisering en interoperabiliteit wordt het internet van de dingen soms gezien als een "*intranet* van de dingen" waarvoor iedere fabrikant zijn eigen interfaces en gegevensformaat heeft vastgesteld. Gegevens worden dan gehost in afgeschermde omgevingen die voorkomen dat gebruikers hun gegevens overbrengen van het ene apparaat naar het andere (of hun gegevens combineren).

Toch versturen veel IoT-apparaten hun gegevens bij uitstek via smartphones en tablets naar het internet. Daarom hebben fabrikanten geleidelijk aan platforms ontwikkeld voor het hosten van de

[16] Met volgapparatuur zouden werkgevers de gezondheid van werknemers in het oog kunnen houden, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health.

gegevens die via zulke verschillende apparaten worden verzameld, teneinde het beheer hiervan te centraliseren en vergemakkelijken.

Zulke platforms kunnen volgens de EU-wetgeving ook worden aangemerkt als voor de verwerking verantwoordelijken, indien de ontwikkeling van zulke diensten met zich meebrengt dat zij de persoonsgegevens van de gebruikers voor hun eigen doeleinden verzamelen.

3.4 **Personen als betrokkenen: abonnees, gebruikers, niet-gebruikers**

Abonnees en gebruikers van het IoT in het algemeen worden uit hoofde van de EU-wetgeving aangemerkt als betrokkenen. Als de gegevens die zij verzamelen en bewaren, uitsluitend worden gebruikt voor persoonlijke of huishoudelijke doeleinden, vallen zij onder de uitzondering voor huishoudens van Richtlijn 95/46/EG[17]. In de praktijk brengt het bedrijfsmodel van het IoT echter met zich mee dat de gegevens van de gebruiker systematisch worden doorgegeven aan fabrikanten van apparaten, ontwikkelaars van toepassingen en andere derde partijen die worden aangemerkt als voor de gegevensverwerking verantwoordelijken. De uitzondering voor huishoudens blijft derhalve beperkt toepasbaar in het kader van het IoT.

De gegevensverwerking in het IoT kan ook betrekking hebben op personen die noch abonnee zijn, noch gebruiker van het IoT. Zo zullen met wearables als intelligente brillen waarschijnlijk ook gegevens worden verzameld over andere betrokkenen dan de eigenaar van het apparaat. Het is belangrijk om te benadrukken dat de EU-wetgeving desondanks onverminderd van toepassing is op dergelijke situaties. De toepasselijkheid van de EU-wetgeving inzakegegevensbescherming is niet afhankelijk van de eigendom van een apparaat of eindapparaat maar van de verwerking van de persoonsgegevens, wie de betrokkene ook is.

4. Verplichtingen van belanghebbenden in het IoT

Belanghebbenden in het IoT die volgens de EU-wetgeving worden aangemerkt als voor de verwerking verantwoordelijken (alleen of samen met anderen), dienen te voldoen aan de verschillende verplichtingen die op hen rusten op grond van Richtlijn 95/46/EG en de betreffende bepalingen van Richtlijn 2002/58/EG, indien van toepassing. In dit advies komt alleen de toepasselijkheid van bepalingen die in dit kader specifieke aandacht verdienen aan de orde, maar dit laat de toepasselijkheid van andere, niet genoemde bepalingen onverlet.

4.1 **Toepasselijkheid van artikel 5, lid 3, van de e-privacyrichtlijn**

Artikel 5, lid 3 van of Richtlijn 2002/58/EG is van toepassing op situaties waarin een belanghebbende bij het IoT toegang krijgt tot informatie, of informatie bewaart, die reeds op een IoT-apparaat is opgeslagen, voor zover IoT-apparaten worden aangemerkt als "eindapparatuur" in de zin van deze bepaling[18]. De bepaling houdt in dat deze handelingen alleen rechtmatig zijn indien de betreffende abonnee of gebruiker in dat geval toestemming geeft voor een dergelijke opslag of toegang, tenzij ze "strikt noodzakelijk zijn om een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst te leveren" [19]. Dit vereiste is met name van belang omdat andere belanghebbenden dan de gebruiker of

[17] Zie advies 5/2009 over online sociale netwerken, goedgekeurd op 12 juni 2009 (WP 163).
[18] Het begrip "eindapparatuur" in artikel 5, lid 3, heeft dezelfde betekenis als "middelen" in artikel 4, lid 1, onder c).
[19] Advies 02/2013 over apps op intelligente apparaten (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_nl.pdf.

abonnee toegang kunnen hebben tot privacygevoelige informatie die op zulke eindapparatuur is opgeslagen[20].

Het vereiste van toestemming in artikel 5, lid 3, heeft hoofdzakelijk betrekking op de fabrikant van het apparaat, maar ook op alle belanghebbenden die toegang wensen tot de geaggregeerde gegevens die in deze infrastructuur zijn opgeslagen. Het is ook van toepassing op iedere voor verwerking verantwoordelijke die aanvullende gegevens op het apparaat van een gebruiker wenst te bewaren.

In voorkomend geval dienen belanghebbenden bij het IoT ervoor te zorgen dat de betrokkene daadwerkelijk toestemming heeft gegeven voor dergelijke opslag en/of toegang, na duidelijk en uitvoerig over onder meer de doeleinden van de verwerking te zijn geïnformeerd door de voor de verwerking verantwoordelijke.

Derhalve dient de toestemming van de gebruiker te worden verkregen voordat de voor de verwerking verantwoordelijke zich toegang verschaft tot apparaatinformatie die kan worden gebruikt om een fingerprint van een apparaat aan te maken (ook wearables). De Groep heeft in werkdocument 02/2013 (WP-208) reeds richtsnoeren aangereikt inzake toestemming voor cookies en soortgelijke traceertechnieken en zal hiervoor verdere richtsnoeren geven in het komende advies over fingerprinting.

Voorbeeld: een stappenteller registreert het aantal stappen dat door zijn gebruiker is gezet en slaat deze informatie op in zijn interne geheugen. De gebruiker installeert een toepassing op zijn computer waarmee hij het aantal stappen direct van zijn apparaat kan downloaden. Om de gegevens van de stappenteller te uploaden naar zijn servers heeft de fabrikant van het apparaat krachtens artikel 5, lid 3, van Richtlijn 2002/58/EG de toestemming van de gebruiker nodig.

Heeft de fabrikant de gegevens eenmaal geüpload, dan bewaart hij alleen de geaggregeerde gegevens over het aantal stappen per minuut. Een toepassing die om toegang tot zulke gegevens verzoekt, voor zover deze niet is opgeslagen op de server van de fabrikant, is dan niet onderhevig aan artikel 5, lid 3, van de e-privacyrichtlijn, maar aan bepalingen van Richtlijn 95/46/EG die betrekking hebben op de rechtmatigheid van deze verdere verwerking.

Bovendien kunnen de eigenaar van een IoT-apparaat en de persoon wiens gegevens worden bijgehouden (de betrokkene) verschillende personen zijn. Deze situatie kan leiden tot een verdeelde toepassing van artikel 5, lid 3, van Richtlijn 2002/58/EG en Richtlijn 95/46/EG.

Voorbeeld: een autoverhuurdienst installeert een intelligent voertuigvolgsysteem in zijn huurauto's. Hoewel de autoverhuurdienst wordt beschouwd als eigenaar/abonnee van het apparaat/volgsysteem, wordt de huurder van de auto aangemerkt als gebruiker van het apparaat. Artikel 5, lid 3, vereist nu dat de fabrikant van het apparaat (ten minste) de toestemming verkrijgt van de gebruiker van het apparaat, in dit geval de huurder van de auto. Bovendien is de rechtmatigheid van de verwerking van de persoonsgegevens van de huurders van de auto's onderhevig aan de bepalingen van artikel 7 van Richtlijn 95/46/EG.

4.2 **Rechtsgrondslag voor de verwerking (artikel 7 van Richtlijn 95/46/EG)**

De verwerking van persoonsgegevens is alleen rechtmatig als belanghebbenden in het IoT die worden aangemerkt als voor de verwerking verantwoordelijken (zie hierboven onder punt 4.3), ervoor zorgen dat aan een van de in artikel 7 van deze richtlijn opgesomde vereisten wordt voldaan. Deze vereisten zijn van toepassing op sommige van deze belanghebbenden, bovenop de toepassing van artikel 5,

[20] Zie overweging 25 van Richtlijn 2002/58/EG.

lid 3, indien de betreffende verwerking verder gaat dan de opslag van, of het toegang krijgen tot informatie die in de eindapparatuur van de gebruiker/abonnee is opgeslagen[21].

In de praktijk zijn hier drie rechtsgrondslagen van belang.

Toestemming (artikel 7, lid a) is de eerste rechtsgrondslag en hierop dient men zich bij het IoT hoofdzakelijk te verlaten, of het nu gaat om fabrikanten van apparaten, sociale en gegevensplatforms, verhuurders van apparaten of ontwikkelaars als derde partij. De Groep heeft meerdere malen richtsnoeren gegeven over de gelijktijdige toepassing van de vereisten van artikel 7, onder a), en artikel 5, lid 3, van Richtlijn 2002/58/EG[22]. De voorwaarden waaronder een dergelijke toestemming volgens de EU-wetgeving geldig is, zijn ook nader bepaald in een eerder advies van de Groep[23].

Artikel 7, onder b), bepaalt ook dat de verwerking rechtmatig is indien deze noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene een partij is. De reikwijdte van deze rechtsgrondslag wordt beperkt door het criterium van "noodzakelijkheid", dat vereist dat er een direct, objectief verband bestaat tussen de verwerking zelf en de doeleinden van de uitvoering van het contract door de betrokkene.

Ten derde staat artikel 7, onder f), de verwerking van persoonsgegevens toe indien de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene — met name diens recht op een persoonlijke levenssfeer met betrekking tot de verwerking van persoonsgegevens — die worden beschermd door artikel 1, lid 1, van deze richtlijn, niet prevaleren.

In zijn arrest in de zaak *Google Spain*[24] heeft het Europese Hof van Justitie belangrijke richtsnoeren geboden voor de interpretatie van deze bepaling, in aanvulling op de richtsnoeren die reeds werden geboden in de voorgaande zaken ASNEF en FECEMD (C-468/10 en C-469/10). In het kader van het IoT heeft de verwerking van de persoonsgegevens van een persoon waarschijnlijk grote invloed op zijn grondrechten op een persoonlijke levenssfeer en de bescherming van persoonsgegevens in situaties waarin gegevens zonder IoT-apparaten niet of slechts met zeer grote moeite met elkaar gecombineerd hadden kunnen worden. Zulke situaties kunnen zich voordoen indien de verzamelde gegevens betrekking hebben op de gezondheid, de huiselijke of de intieme sfeer, de locatie en vele andere aspecten van het privéleven van de betrokkene. Gezien de mogelijke ernst van die inmenging is het duidelijk dat een dergelijk verwerking nauwelijks te rechtvaardigen is door louter het economische belang dat een belanghebbende bij het IoT heeft bij deze verwerking. Andere belangen die worden nagestreefd door de voor de verwerking verantwoordelijke of door de derde partij(en) waaraan de gegevens worden onthuld, dienen hierbij een rol te spelen[25].

---

[21] Over de verwoording van artikel 5, lid 3, en artikel 7, onder a), zie met name Advies 02/2013 betreffende apps op intelligente apparaten, goedgekeurd op 27 februari 2013 (WP202) – (blz. 14 e.v.), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_nl.pdf en Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG (WP217) – (blz. 26, 32, 46).

[22] Advies WP202, blz.14 e.v.

[23] Advies 15/2011 van de Artikel 2011-Groep over de definitie van toestemming, goedgekeurd op 3 juli 2011 (WP187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_nl.pdf.

[24] Arrest van het Hof (Grote kamer), van 13 mei 2014, in zaak C-131/12 (punt 74 e.v.).

[25] Advies WP217.

Voorbeeld: in het kader van een plan om het gebruik van het openbaar vervoer te bevorderen en vervuiling te verminderen, wil de gemeenteraad het parkeren in de stad reguleren door toegangsbeperkingen op te leggen en parkeergelden te heffen. Het parkeertarief hangt af van verschillende variabelen, waaronder het type motor (diesel, benzine, elektrisch) en de ouderdom van het voertuig. Wanneer een voertuig een onbezette parkeerplaats nadert, kan een sensor de kentekenplaat aflezen en na doorzoeking van een gegevensbank bepalen of er een automatische toepassing van een toeslag of korting volgt volgens vooraf bepaalde criteria. In dit geval zou de verwerking van de kentekengegevens om het tarief te bepalen in dienst kunnen staan van het rechtmatige belang van de voor de verwerking verantwoordelijke. Voor verdere verwerking, zoals het vergaren van – ongeanonimiseerde – informatie over de verplaatsing van voertuigen door het beperkt toegankelijke gebied, zou een andere rechtsgrondslag nodig zijn.

4.3 **Beginselen betreffende de kwaliteit van de gegevens**

Gezamenlijk vormen de beginselen die in artikel 6 van Richtlijn 95/4/EG zijn vastgelegd de hoeksteen van het EU-recht op het gebied van gegevensbescherming.

Persoonsgegevens dienen op eerlijke eerlijke en rechtmatige wijze te worden verzameld en verwerkt. Het eerlijkheidsbeginsel vereist specifiek dat persoonsgegevens nooit worden verzameld en verwerkt zonder dat de persoon zich ervan bewust is. Dit vereiste is des te belangrijker in relatie tot het IoT, omdat sensoren juist zijn ontworpen om zo onopvallend – d.w.z. zo min mogelijk zichtbaar – te functioneren. Toch moeten voor de verwerking verantwoordelijken die actief zijn in het kader van het IoT (voornamelijk fabrikanten van apparaten) iedere persoon in de geografische of digitale nabijheid van onlineapparaten op de hoogte stellen wanneer er gegevens worden verzameld die aan hen of hun omgeving gerelateerd zijn. Naleving van deze bepaling is méér dan een streng wettelijk voorschrift: dat gegevens op eerlijke wijze worden verzameld, behoort tot de meest cruciale verwachtingen die gebruikers hebben van het IoT, met name in het geval van wearables.

Voorbeeld: een gezondheidsgerelateerd apparaat gebruikt een lampje om bij te houden hoe bloed door aderen stroomt en hieruit informatie over de hartslag af te leiden. Het apparaat omvat ook nog een andere sensor die het zuurstofgehalte van het bloed meet, maar er wordt noch op het apparaat noch op de gebruikersinterface informatie gegeven over deze gegevensverzameling. Ook indien de sensor voor het zuurstofgehalte van het bloed volledig functioneel is, dient deze niet te worden ingeschakeld zonder voorafgaande toestemming van de gebruiker. Voor de inschakeling van deze sensor is uitdrukkelijke toestemming vereist.

Het doelbindingsbeginsel houdt in dat gegevens alleen kunnen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Iedere verwerking die strijdig zou zijn met deze oorspronkelijke doeleinden is illegaal volgens het EU-recht. Dit beginsel moet gebruikers in staat stellen zich op de hoogte te stellen van de manier waarop en de doeleinden waarvoor hun gegevens worden gebruikt en te beslissen of ze een voor de verwerking verantwoordelijke hun gegevens toevertrouwen. Deze doeleinden moeten worden gedefinieerd *voordat* de gegevensverwerking plaatsvindt, hetgeen plotselinge veranderingen in de essentiële voorwaarden van de verwerking uitsluit. Dit betekent dat belanghebbenden bij het IoT een goed overzicht van hun businesscase moeten hebben voordat ze beginnen met het verzamelen van persoonsgegevens.

Ook dienen gegevens over de betrokkene strikt noodzakelijk te zijn voor het specifieke doeleinde dat vooraf bepaald is door de voor de verwerking verantwoordelijke (het beginsel van "minimale gegevensverwerking"). Gegevens die voor dit doel niet nodig zijn mogen niet worden verzameld en

opgeslagen "voor het geval dat" of omdat deze "later van pas kunnen komen". Sommige belanghebbenden zijn van mening dat het beginsel van minimale gegevensverwerking de mogelijkheden van het IoT kan beperken en innovatie in de weg kan staan, ervan uitgaande dat de mogelijke voordelen van gegevensverwerking voortkomen uit verkennende analyse van niet voor de hand liggende correlaties en tendensen. De Groep onderschrijft deze analyse niet en stelt nadrukkelijk dat het beginsel van minimale gegevensverwerking een essentiële rol speelt bij de gegevensbescherming waar personen recht op hebben krachtens EU-wetgeving en dat het beginsel als zodanig in acht dient te worden genomen[26]. Uit dit principe volgt dat, indien de persoonsgegevens niet nodig zijn om een specifieke dienst op het IoT te leveren, de betrokkenen ten minste de mogelijkheid moet worden geboden om de dienst anoniem te gebruiken.

Artikel 6 vereist eveneens dat persoonsgegevens die in de context van het IoT worden verzameld en verwerkt, niet langer worden bewaard dan nodig voor het doeleinde waarvoor de gegevens werden verzameld of verder verwerkt. Deze noodzakelijkheidstoets dient te worden uitgevoerd door iedere belanghebbende bij het verlenen van een specifieke dienst op het IoT, daar de doeleinden van hun respectieve verwerkingen verschillend kunnen zijn. Zo moeten persoonsgegevens die een gebruiker heeft opgegeven toen hij zich abonneerde op een bepaalde IoT-dienst , worden verwijderd zodra de gebruiker dit abonnement beëindigt. Evenzo mag informatie die de gebruiker uit zijn account verwijdert, niet worden aangehouden. Als een gebruiker de dienst of toepassing voor een bepaalde tijd niet gebruikt, moet het gebruikersprofiel op inactief worden gezet. Na nog een tijdsperiode dienen de gegevens te worden verwijderd. Voordat de belanghebbende deze stappen neemt, dient hij alles in het werk te stellen om de gebruiker hierover te informeren.

4.4 **Verwerking van gevoelige gegevens (artikel 8)**

Bij IoT-toepassingen kunnen persoonsgegevens worden verwerkt waaruit informatie kan worden afgeleid inzake ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen, vakbondslidmaatschap, gezondheid of het seksuele leven onthullen; dit zijn "gevoelige gegevens" die bijzondere bescherming verdienen in de zin van artikel 8 van Richtlijn 95/46/EG. In de praktijk houdt de toepassing van artikel 8 op gevoelige gegevens op het IoT in dat voor de verwerking verantwoordelijken de uitdrukkelijke toestemming van de gebruiker dienen te verkrijgen, tenzij de betrokkene de gegevens zelf openbaar heeft gemaakt.

In het specifieke kader van bijvoorbeeld apparaten voor zelfkwantificatie is het waarschijnlijk dat een dergelijke situatie zich voordoet. Hierbij gaat het om apparaten die vooral gegevens over het welzijn van de persoon verzamelen. Deze gegevens vertegenwoordigen geen gezondheidsinformatie als zodanig, maar kunnen heel gemakkelijk informatie bieden over de gezondheid van de persoon, aangezien de gegevens door de tijd heen worden geregistreerd, waardoor het mogelijk is om conclusies ter verbinden aan de veranderingen gedurende een bepaalde tijdsperiode. Voor de verwerking verantwoordelijken dienen er rekening te houden met dat de aard van de verwerking in deze zin verschuift en adequate maatregelen te nemen.

Voorbeeld: Bedrijf X heeft een toepassing ontwikkeld die middels de analyse van ruwe gegevens van elektrocardiogramsignalen, gegenereerd door commerciële sensoren die algemeen verkrijgbaar zijn voor consumenten, drugsverslavingen kan opsporen. De engine van de toepassing is in staat om

[26] Verkennend onderzoek wordt in ieder geval nooit op geheel willekeurige wijze uitgevoerd: de algemene doelstelling van een onderzoek wordt van oudsher alleen al om organisatorische en budgettaire redenen ten minste gedeeltelijk gedefinieerd. Het is moeilijk voor te stellen dat de gegevensverwerking voor een specifiek onderzoek nog in overeenstemming zal zijn met het oorspronkelijke doeleinde van de gegevensverzameling; als het doeleinde is veranderd, strookt de gegevensverwerking niet met het EU-recht.

specifieke aspecten van ruwe ecg-gegevens te extraheren die volgens eerdere onderzoeksresultaten gerelateerd zijn aan de consumptie van verdovende middelen. Het product, dat compatibel is met de meeste sensoren op de markt, kan worden gebruikt als zelfstandige toepassing of via een webgebaseerde interface waarvoor de gegevens moeten worden geüpload. Uitdrukkelijke toestemming van de gebruiker is vereist voor de verwerking van de gegevens voor dit doeleinde. Aan dit vereiste van toestemming kan worden voldaan onder dezelfde voorwaarden en op hetzelfde moment als aan de toestemming vereist door artikel 7, onder a).

4.5 **Transparantievereisten (artikelen 10 en 11)**

Behalve het vereiste van eerlijke gegevensverzameling van artikel 6, onder a), moeten voor de verwerking verantwoordelijken krachtens de artikelen 10 en 11 specifieke informatie mededelen aan betrokkenen: de identiteit van de voor de verwerking verantwoordelijke, de doeleinden van de verwerking, de ontvangers van de gegevens, het bestaan van hun rechten op toegang en hun recht van bezwaar (waaronder informatie over hoe de verbinding van het apparaat kan worden verbroken om te voorkomen dat meer gegevens onthuld worden).

Afhankelijk van de toepassing kan deze informatie bijvoorbeeld worden vermeld op het voorwerp zelf, worden verstuurd via de draadloze verbinding, of met gebruikmaking van de locatie – door middel van nabijheidstests voor de bescherming van de persoonlijke levenssfeer die door een gecentraliseerde server worden uitgevoerd – waarbij gebruikers die zich dichtbij de sensor bevinden hiervan op de hoogte worden gesteld.

Verder moet deze informatie in overeenstemming met het beginsel van eerlijke verwerking op een duidelijke wijze kenbaar worden gemaakt. De fabrikant van het apparaat zou bijvoorbeeld op dingen die van sensoren zijn voorzien een QR-code of flashcode kunnen drukken die het type sensor en het type geregistreerde informatie beschrijft, alsook de doelen van de gegevensverzameling.

4.6 **Beveiliging (artikel 17)**

Artikel 17 van de privacyrichtlijn bepaalt dat de voor de verwerking verantwoordelijke „passende technische en organisatorische maatregelen ten uitvoer dient te leggen om persoonsgegevens te beveiligen" en dat „de voor de verwerking verantwoordelijke, in geval van verwerking te zijnen behoeve, een verwerker moet kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking".

Derhalve blijft een belanghebbende die wordt aangemerkt als voor de verwerking verantwoordelijke volledig verantwoordelijk voor de beveiliging van de gegevensverwerking. Indien zwakke plekken in de beveiliging die leiden tot inbreuken op de beveiliging het resultaat zijn van gebrekkig ontwerp of onderhoud van de gebruikte apparaten, is de voor de verwerking verantwoordelijke aansprakelijk. Voor de verwerking verantwoordelijken dienen daarom veiligheidsbeoordelingen te verrichten van de systemen als geheel, ook op het niveau van de onderdelen, waarbij beginselen van configureerbare beveiliging ("composable security") worden toegepast. Evenzo dient het gebruik van certificatie van apparaten alsmede de afstemming op internationaal erkende beveiligingsnormen te worden geïmplementeerd om de algehele beveiliging van het IoT te verbeteren.

Subcontractanten die hardware-onderdelen ten behoeve van andere belanghebbenden ontwerpen en vervaardigen zonder persoonsgegevens te verwerken, kunnen strikt genomen niet aansprakelijk worden gehouden op grond van artikel 17 van Richtlijn 95/46/EG in geval van een inbreuk op de gegevensbescherming ten gevolge van een gebrek in de beveiliging van deze apparaten. Deze belanghebbenden vervullen echter een essentiële rol in de beveiliging van het IoT-ecosysteem. Belanghebbenden die directe verantwoordelijkheden voor gegevensbescherming dragen jegens

betrokkenen, dienen ervoor te zorgen dat deze subcontractanten bij het ontwerp en de vervaardiging van hun producten gehouden zijn aan hoge beveiligingsnormen met betrekking tot de persoonlijke levenssfeer.

Zoals gezegd dienen er veiligheidsmaatregelen te worden genomen met inachtneming van de specifieke operationele beperkingen van IoT-apparaten. Zo kunnen de meeste huidige sensoren geen versleutelde verbinding leggen, omdat voorrang wordt gegeven aan de fysieke autonomie van het apparaat of aan kostenbeheersing.

Bovendien zijn apparaten die functioneren in het IoT ook moeilijk te beveiligen, zowel om technische als bedrijfseconomische redenen. Omdat de onderdelen ervan doorgaans gebruik maken van draadloze communicatie-infrastructuur en worden gekenmerkt door beperkte energie en rekenkracht, zijn de apparaten kwetsbaar voor fysieke aanvallen, afluisteren of aanvallen via proxy's. De meeste gangbare technologieën die momenteel in gebruik zijn – PKI-infrastructuren – zijn niet eenvoudig te poorten op apparaten voor het IoT, aangezien de meeste apparaten niet beschikken over de rekenkracht die benodigd is voor de vereiste verwerkingen. Het IoT behelst een complexe toeleveringsketen met meerdere belanghebbenden, die ieder in verschillende mate verantwoordelijkheden op zich nemen. Een beveiligingsinbreuk kan bij ieder van hen ontstaan zijn, vooral in M2M-omgevingen op basis van gegevensuitwisseling tussen apparaten. Derhalve dient rekening te worden gehouden met de behoefte aan veilige en lichte protocollen die kunnen worden gebruikt in omgevingen met beperkte energie en rekenkracht.

De Groep benadrukt dat het in deze omstandigheden, waarin beperkte rekencapaciteit een risico kan vormen voor veilige en efficiënte communicatie, nog belangrijker is om het beginsel van minimale gegevensverwerking in acht te nemen en de verwerking van persoonsgegevens, met name de opslag ervan op het apparaat, te beperken tot het benodigde minimum.

Bovendien worden apparaten die zijn ontworpen voor directe toegankelijkheid via internet, niet altijd door de gebruiker ingesteld. Daardoor kunnen ze een eenvoudige toegangsweg vormen voor indringers als ze worden gebruikt met de standaardinstellingen. Beveiligingspraktijken op basis van de beperking van toegang tot het netwerk, de uitschakeling per standaardinstelling van niet-kritieke functionaliteiten en het voorkomen van het gebruik van niet-vertrouwde bronnen van software-updates (ter beperking van malware-aanvallen op basis van codewijziging), kunnen bijdragen aan het beperken van de invloed en omvang van mogelijke gegevensinbreuken. Zulke bescherming van de persoonlijke levenssfeer dient al in het eerste stadium te worden ingebouwd, overeenkomstig het beginsel "Privacy by Design".

Daarnaast leidt het gebrek aan automatische updates tot een grote hoeveelheid nog niet verholpen kwetsbaarheden, die met gespecialiseerde zoekmachines eenvoudig te ontdekken zijn. Zelfs in de gevallen waarin de gebruikers zich bewust zijn van kwetsbaarheden die van invloed zijn op hun eigen apparaten, hebben ze mogelijk geen toegang tot de updates van de leverancier, hetzij door hardwarebeperkingen, hetzij doordat het apparaat als gevolg van verouderde technologieën software-updates niet ondersteunt. Mocht een fabrikant van een apparaat de ondersteuning van een apparaat staken, dan moeten alternatieve oplossingen worden geleverd om deze te ondersteunen (bv. de software ter beschikking stellen aan de opensourcegemeenschap). Gebruikers moeten ervan op de hoogte worden gesteld dat hun apparaten waarschijnlijk kwetsbaar zullen zijn vanwege nog niet verholpen gebreken.

Sommige commerciële zelfmeetsystemen (bv. stappentellers, slaapmeters) vertonen eveneens zwakke plekken in de beveiliging, die aanvallers kunnen uitbuiten om gemeten waarden te vervalsen die aan

de fabrikanten van toepassingen en apparaten worden gemeld. Het is van essentieel belang dat deze apparaten adequate bescherming bieden tegen gegevensvervalsing, met name als de door deze sensoren gemeten waarden indirect invloed hebben op de beslissingen van gebruikers op het gebied van gezondheid.

Een adequaat beleid voor de melding van gegevensinbreuken kan ook de negatieve effecten van kwetsbaarheden van ontwerp en software helpen beperken door het verspreiden van kennis en het aanreiken van richtsnoeren terzake.

5. Rechten van de betrokkene

Belanghebbenden bij het IoT dienen de rechten van betrokkenen te respecteren conform de artikelen 12 en 14 van Richtlijn 95/46/EG en dienovereenkomstig maatregelen te treffen. Deze rechten komen niet alleen toe aan de abonnees op IoT-diensten of gebruikers van IoT-apparaten , maar aan iedere persoon van wie gegevens worden verwerkt.

5.1 **Recht van toegang**

Artikel 12, onder a), bepaalt dat betrokkenen er recht op hebben dat voor de verwerking verantwoordelijken op inzichtelijke wijze aan hen mededelen welke gegevens onderwerp zijn van verwerking en hun alle beschikbare informatie verstrekken over de oorsprong van deze gegevens.

In de praktijk zijn gebruikers van het IoT vaak gebonden aan bepaalde systemen. Gegevens worden doorgaans eerst naar de fabrikant gestuurd, die deze vervolgens via een webportaal of app toegankelijk maakt voor de gebruiker. Deze opzet stelt fabrikanten in staat om onlinediensten te leveren waardoor de gebruiksmogelijkheden van het apparaat worden vergroot, maar kan ook beletten dat gebruikers de dienst voor de interactie met hun apparaat vrijelijk kiezen.

Bovendien zijn eindgebruikers zelden in staat om toegang te krijgen tot de ruwe gegevens verzameld door IoT-apparaten. Ze stellen duidelijk een groter direct belang in de geïnterpreteerde gegevens dan in de ruwe gegevens, die zij mogelijk niet begrijpen. Toegang tot zulke gegevens kan evenwel nuttig zijn voor de eindgebruikers om inzicht te krijgen in hetgeen de fabrikant daaruit over hen kan afleiden. Ook kan de beschikking over deze ruwe gegevens gebruikers de mogelijkheid geven hun gegevens over te dragen aan een andere verantwoordelijke voor gegevensverwerking – bijvoorbeeld als de oorspronkelijk voor de verwerking verantwoordelijke zijn privacybeleid op een onbevredigende wijze verandert. Op dit moment hebben deze personen praktisch geen andere optie dan te stoppen met het gebruik van hun apparaten, omdat de meeste voor de verwerking verantwoordelijken een dergelijke functionaliteit niet bieden en alleen toegang bieden tot een inferieure versie van de opgeslagen gegevens.

De Groep is van mening dat een dergelijke opstelling een belemmering vormt voor de effectieve uitoefening van het recht van toegang, aan personen toegekend door artikel 12, onder a), van Richtlijn 95/46/EG. De Groep meent dat belanghebbenden bij het IoT maatregelen moeten nemen om gebruikers in staat te stellen dit recht effectief uit te oefenen en ze de mogelijkheid te geven een andere dienst te kiezen die mogelijk niet door de fabrikant als optie wordt voorgesteld. Het ontwikkelen van normen voor de interoperabiliteit van gegevens kan hieraan een nuttige bijdrage leveren.

Zulke maatregelen zijn des te belangrijker omdat het zogenoemde "recht van gegevensoverdraagbaarheid", dat in het concept van de algemene verordening gegevensbescherming waarschijnlijk zal worden vastgelegd als variant van het recht van toegang, ten doel heeft een het

afhankelijk maken van gebruikers ("user lock-in") uit te bannen[27]. Het streven van de Europese wetgever bestaat erin om obstakels voor concurrentie weg te nemen en nieuwe spelers te helpen innoveren op deze markt.

5.2 **Mogelijkheid tot intrekking van toestemming en tot aantekening van bezwaar**

Betrokkenen dienen de mogelijkheid te hebben om vooraf gegeven toestemming voor een specifieke gegevensverwerking in te trekken en om bezwaar te maken tegen de op hen betrekking hebbende gegevensverwerking. Dergelijke rechten moeten kunnen worden uitgeoefend zonder enige technische of organisatorische beperkingen of hindernissen en de hulpmiddelen voor de registratie van deze intrekking dienen toegankelijk, zichtbaar en doelmatig te zijn.

Systemen voor intrekken moeten specifiek zijn en betrekking hebben op: 1) alle gegevens die zijn verzameld door een specifiek ding (een gebruiker moet bv. kunnen instellen dat het weerstation stopt met de verzameling van gegevens over vochtigheid, temperatuur en geluiden); 2) specifieke typen gegevens verzameld door welk apparaat dan ook (een gebruiker moet bv. de gegevensverzameling kunnen onderbreken van ieder apparaat dat geluid registreert, of het nu gaat om een slaapmeter of een weerstation); 3) specifieke gegevensverwerkingen (een gebruiker moet er bv. voor kunnen zorgen dat zowel zijn stappenteller als horloge stoppen met het tellen van zijn stappen).

Aangezien wearables waarschijnlijk ter vervanging zullen dienen van de bestaande niet-onlineartikelen met de gebruikelijke functionaliteiten, dienen voor de verwerking verantwoordelijken tevens een optie aan te bieden voor het uitschakelen van de onlinefunctionaliteit van het voorwerp om het te laten functioneren als het oorspronkelijke niet-onlineartikel.. De Groep heeft reeds gesteld dat de betrokkene de volgende mogelijkheid moet hebben: „De gebruiker kan zijn of haar toestemming voortdurend intrekken, zonder dat hij of zij hoeft te stoppen met het gebruik" van de geleverde dienst[28].

Voorbeeld: een gebruiker installeert een onlinebrandmelder in zijn appartement. Het alarm maakt gebruik van een aanwezigheidssensor, een warmtesensor en een lichtsensor. Sommige van deze sensoren zijn nodig voor de branddetectie, terwijl andere alleen aanvullende functies bieden waarover de gebruiker vooraf was geïnformeerd. De gebruiker moet deze functies kunnen uitschakelen om alleen het brandalarm te kunnen gebruiken en dus de voor deze functies gebruikte sensoren kunnen uitschakelen.

Interessant is dat bij sommige recente ontwikkelingen op dit gebied de betrokkenen de regie in handen wordt gegeven, in de vorm van controle over de functies voor toestemmingsbeheer, bijvoorbeeld middels sticky policy's[29] of privacy proxy's[30].

---

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf.

[28] Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, goedgekeurd op 16 mei 2011 (WP185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_nl.pdf.

[29] In dat opzicht kan een benadering op basis van zogenoemde sticky policy's de naleving van het kader voor gegevensbescherming ondersteunen door informatie over voorwaarden en beperkingen van het gegevensgebruik in te sluiten in de gegevens zelf. Zo zouden in deze policy's dus de context van het gegevensgebruik, de doeleinden, het beleid voor toegang van derde partijen en een lijst van betrouwbare gebruikers kunnen worden vastgelegd.

[30] Een manier om betrokkenen reële controle te bieden over de manier waarop gegevens worden verwerkt bij de interactie met sensoren − waarbij ze in staat worden gesteld om voorkeuren aan te geven, waaronder keuzes voor het geven of intrekken van toestemming en voor het beperken van doeleinden − kan worden gebaseerd op het gebruik van privacyproxy's. Bij ondersteuning door een apparaat worden gegevensaanvragen worden

6. Conclusies en aanbevelingen

Hieronder volgt een aantal aanbevelingen die de Groep als nuttig beschouwt om het gemakkelijker te maken de hierboven opgesomde wettelijke vereisten van de EU toe te passen op het IoT.

Deze aanbevelingen behelzen alleen richtsnoeren die een aanvulling vormen op eerder door de Groep goedgekeurde documenten.

Wat dat betreft wil de Groep in het bijzonder wijzen op de eerdere aanbevelingen inzake apps op intelligente apparaten[31]. Omdat smartphones onderdeel zijn van de IoT-omgeving en bij beide ecosystemen een vergelijkbare groep belanghebbenden betrokken is, zijn deze aanbevelingen relevant voor het IoT. Met name dienen ontwikkelaars van apps en fabrikanten van apparaten eindgebruikers adequaat te informeren en eenvoudige opt-outs en/of gespecificeerde toestemming aan te bieden, indien van toepassing. Indien geen toestemming is gegeven, dient de voor de verwerking verantwoordelijke de gegevens bovendien te anonimiseren alvorens deze voor een andere bestemming aan te wenden of te delen met andere partijen.

6.1 **Aanbevelingen aan alle belanghebbenden**

- Er zouden Privacy Impact Assessments (PIA's, privacyeffectbeoordelingen) moeten worden verricht voordat het IoT wordt uitgebreid met nieuwe toepassingen. De te volgen methode voor deze PIA's kan worden gebaseerd op het kader voor effectbeoordelingen inzake bescherming van gegevens en de persoonlijke levenssfeer, door de Groep op 12 januari 2011 goedgekeurd voor RFID-toepassingen[32]. Indien passend/haalbaar dienen belanghebbenden te overwegen de relevante PIA algemeen beschikbaar te maken. Er kunnen gespecificeerde PIA-kaders worden ontwikkeld voor bepaalde IoT -ecosystemen (bv. intelligente steden).

- Menig belanghebbende bij het IoT heeft alleen geaggregeerde gegevens nodig en geen ruwe gegevens verzameld door IoT-apparaten. Belanghebbenden dienen ruwe gegevens te verwijderen zodra ze de voor hun gegevensverwerking benodigde gegevens hebben geëxtraheerd. In beginsel dient de verwijdering zo dicht mogelijk bij het punt van verzameling van de ruwe gegevens plaats te vinden (bv. op hetzelfde apparaat na verwerking).

- Iedere belanghebbende in het IoT zou de beginselen "Privacy by Design" (privacy door ontwerp) en "Privacy by Default" (privacy door standaardinstellingen) moeten toepassen.

- "User empowerment" − de gebruiker de regie in handen geven − is essentieel voor het IoT. Betrokkenen en gebruikers moeten in staat zijn om hun rechten uit te oefenen en dus, overeenkomstig het beginsel van informationele zelfbeschikking, op ieder moment controle over hun gegevens hebben.

- De methoden voor het geven van informatie, het bieden van de optie om te weigeren en het vragen van toestemming dienen zo gebruiksvriendelijk mogelijk te zijn. Met name beleid voor informering en toestemming dient gericht te zijn op informatie die voor de gebruiker begrijpelijk is en niet beperkt te blijven tot een algemeen privacybeleid op de internetpagina van de voor de verwerking verantwoordelijke.

---

geconfronteerd met vooraf vastgesteld beleid over de toegang tot de door de betrokkene beheerde gegevens . Door sensoren te koppelen aan policy's zouden aanvragen van derde partijen voor de verzameling van of toegang tot sensorgegevens worden toegewezen, in beperkte mate worden toegewezen of worden afgewezen.

[31] Advies 02/2013 over apps op intelligente apparaten (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_nl.pdf.

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf.

- Apparaten en toepassingen moeten ook worden ontworpen om gebruikers en andere betrokkenen te informeren, bijvoorbeeld middels de fysieke interface van het apparaat of door een signaal te verzenden over een draadloos kanaal.

6.2 Fabrikanten van besturingssystemen en apparaten

- Fabrikanten van apparaten moeten gebruikers informeren over het type gegevens dat wordt verzameld door sensoren en verder wordt verwerkt, de typen gegevens die ze ontvangen en de wijze waarop ze worden verwerkt en gecombineerd.

- Fabrikanten van apparaten moeten in staat zijn om, zodra een betrokkene zijn toestemming intrekt of bezwaar maakt tegen de gegevensverwerking, dit aan alle andere belanghebbenden mee te delen.

- Fabrikanten van apparaten moeten specifieke keuzen bieden bij het verlenen van toegang tot toepassingen. De specificiteit dient niet alleen de categorieën verzamelde gegevens te betreffen, maar ook de tijdstippen en frequentie waarop gegevens worden geregistreerd. Zoals smartphones een functie "niet storen" hebben, dient er op IoT-apparaten een optie "niet verzamelen" te worden aangeboden om de werking van sensoren te programmeren of vlug uit te schakelen.

- Om locatieopsporing te voorkomen, dienen fabrikanten van apparaten device fingerprinting te beperken door draadloze interfaces uit te schakelen wanneer ze niet worden gebruikt of door willekeurige identificatoren te gebruiken (zoals willekeurige MAC-adressen om WiFi-netwerken te scannen).

- Om transparantie en zeggenschap van de gebruiker te handhaven dienen fabrikanten van apparaten hulpmiddelen te bieden voor het lokaal lezen, bewerken en wijzigen van de gegevens voordat deze worden doorgegeven aan een voor de verwerking verantwoordelijke. Verder dienen persoonsgegevens die door een apparaat worden verwerkt, te worden opgeslagen in een formaat dat overdraagbaarheid mogelijk maakt.

- Gebruikers hebben recht van toegang tot hun persoonsgegevens. Ze moeten worden voorzien van hulpmiddelen waarmee ze hun gegevens eenvoudig kunnen exporteren in een gestructureerd en gangbaar formaat. Derhalve dienen fabrikanten van apparaten een gebruiksvriendelijke interface aan te bieden voor gebruikers die geaggregeerde en/of ruwe gegevens willen verkrijgen die zij nog bewaren.

- Fabrikanten van apparaten dienen eenvoudige hulpmiddelen te bieden om gebruikers op de hoogte te stellen en apparaten te updaten wanneer er kwetsbare punten in de beveiliging zijn ontdekt. Wanneer een apparaat wordt afgeschaft en niet meer geüpdatet zal worden, moet de fabrikant de gebruiker hiervan op de hoogte stellen en zich ervan vergewissen dat deze weet dat het apparaat niet meer geüpdatet zal worden. Alle belanghebbenden die waarschijnlijk gevolgen zullen ondervinden van het kwetsbare punt, moeten eveneens op de hoogte worden gesteld.

- Fabrikanten dienen een proces van security-by-design te volgen en enkele componenten te wijden aan de belangrijkste cryptografische primitieven.

- Fabrikanten dienen de hoeveelheid gegevens die het apparaat kunnen verlaten, zoveel mogelijk te beperken door ruwe gegevens onmiddellijk op het apparaat in geaggregeerde gegevens om te zetten. Geaggregeerde gegevens moeten een gestandaardiseerd formaat hebben.

- In tegenstelling tot smartphones kunnen IoT-apparaten worden gedeeld door meerdere betrokkenen en zelfs worden verhuurd (bv. intelligente huizen). Er moet een instelling beschikbaar zijn om onderscheid te kunnen maken tussen verschillende personen die hetzelfde apparaat gebruiken, zodat zij geen informatie krijgen over elkaars activiteiten.

- Fabrikanten zouden met normalisatie-instellingen en gegevensplatforms moeten samenwerken om een gemeenschappelijk protocol te ondersteunen voor de uiting van voorkeuren met betrekking tot gegevensverzameling en de verwerking door voor de verwerking verantwoordelijken, met name indien deze gegevens worden verzameld door onopvallende apparaten.

- Fabrikanten zouden lokale voor de verwerking verantwoordelijke en verwerkende entiteiten mogelijk moeten maken ("personal privacy proxies"), waardoor gebruikers een duidelijk beeld kunnen krijgen van de door hun apparaten verwerkte gegevens, en die lokale opslag en verwerking vergemakkelijken zonder dat de gegevens hoeven te worden doorgegeven aan de fabrikant van het apparaat.

6.3 **Ontwikkelaars van toepassingen**

- Er zouden berichten ter kennisgeving of waarschuwing moeten worden ontworpen om gebruikers er frequent aan te herinneren dat sensoren gegevens verzamelen. Indien de ontwikkelaar van de toepassing geen directe toegang tot het apparaat heeft, moet de app de gebruiker regelmatig berichten dat er nog steeds gegevens worden geregistreerd.

- Toepassingen zouden betrokkenen in staat moeten stellen hun rechten van toegang, wijziging en verwijdering van door IoT-apparaten verzamelde persoonsgegevens uit te oefenen.

- Ontwikkelaars van toepassingen moeten hulpmiddelen bieden waarmee betrokkenen zowel ruwe als geaggregeerde gegevens naar een standaard en bruikbaar formaat kunnen exporteren.

- Ontwikkelaars dienen bijzondere aandacht te schenken aan de typen gegevens die worden verwerkt en aan de mogelijkheid dat hieruit persoonsgegevens worden afgeleid.

- Ontwikkelaars van toepassingen zouden het beginsel van minimale gegevensverwerking moeten toepassen. Als het doeleinde kan worden bereikt met gebruikmaking van geaggregeerde gegevens, zouden ontwikkelaars geen toegang moeten hebben tot de ruwe gegevens. Meer in het algemeen moeten ontwikkelaars uitgaan van privacy-by-design en niet meer gegevens verzamelen dan nodig is voor om de dienst te verlenen.

6.4 **Sociale platforms**

- Tot de standaardinstellingen van sociale toepassingen op basis van IoT-apparaten zou moeten behoren dat aan gebruikers de keuze wordt voorgelegd om informatie te herzien of bewerken of erover te beslissen, voordat deze wordt gepubliceerd op sociale platforms.

- Informatie die door IoT-apparaten op sociale platforms is gepubliceerd, zou per standaardinstelling niet openbaar moeten worden gemaakt en niet worden geïndexeerd door zoekmachines.

6.5 **Eigenaren van IoT-apparaten en verdere ontvangers**

- Toestemming tot het gebruik van een onlineapparaat en tot de hieruit voortvloeiende gegevensverwerking moet berusten op informatie en vrijelijk worden gegeven. Gebruikers mogen niet

in economisch opzicht worden benadeeld en ook de toegang tot functies van hun apparaten mag niet worden beperkt, indien ze besluiten het apparaat of een specifieke dienst niet te gebruiken.

- De betrokkene wiens gegevens worden verwerkt in het kader van een contractuele relatie met de gebruiker van een onlineapparaat (bv. hotel, zorgverzekeraar of autoverhuurder), zou de mogelijkheid moeten hebben het apparaat te beheren. Ongeacht of er sprake is van een contractuele relatie zou iedere betrokkene die geen gebruiker is, in staat moeten worden gesteld om zijn rechten van toegang en bezwaar uit te oefenen.

- Gebruikers van IoT-apparaten zouden betrokkenen wier gegevens worden verzameld en die geen gebruiker zijn, op de hoogte moeten stellen van de aanwezigheid van IoT-apparaten en van het type gegevens dat wordt verzameld. Ook zouden zij gehoor moeten geven aan de wens van betrokkenen die niet willen dat hun gegevens door het apparaat worden verzameld.

6.6 **Normalisatie-instellingen en gegevensplatforms**

- Normalisatie-instellingen en gegevensplatforms zouden gegevensformaten moeten bevorderen die draagbaar, interoperabel alsook helder zijn en die geen uitleg behoeven, om de doorgifte van gegevens tussen verschillende partijen te faciliteren en om betrokkenen te helpen inzicht te krijgen in welke gegevens over hen worden verzameld door IoT-apparaten.

- Normalisatie-instellingen en gegevensplatforms zouden niet alleen gericht moeten zijn op het formaat voor ruwe gegevens, maar ook op de opkomst van formaten voor geaggregeerde gegevens.

- Normalisatie-instellingen en gegevensplatforms zouden gegevensformaten moeten bevorderen die een zo klein mogelijk aantal sterke identificatoren bevatten, zodat IoT-gegevens naar behoren kunnen worden geanonimiseerd.

- Normalisatie-instellingen zouden moeten werken aan gecertificeerde normen als toetssteen voor het waarborgen van de veiligheid en de persoonlijke levenssfeer van betrokkenen.

- Normalisatie-instellingen zouden specifiek voor het IoT lichte versleutelings- en communicatieprotocollen moeten ontwikkelen om vertrouwelijkheid, integriteit, authenticatie en toegangscontrole te garanderen.