PERSOONSGEGEVEN

In deze factsheet komen de volgende onderwerpen aan bod:

DEFINITIE

Op dit moment geldt de definitie uit de Europese Privacy Richtlijn zoals geïmplementeerd in de Wbp.

WBP: Artikel 1, aanhef en onder a Wbp
Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Artikel 16 Wbp bepaalt van de daar genoemde specifieke persoonsgegevens dat sprake is van "*bijzondere persoonsgegevens*" waarvoor een verwerkingsverbod geldt.

Richtlijn: Artikel 2 onder a van de Europese Richtlijn bescherming persoonsgegevens (Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995)
(a) Persoonsgegeven: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene" te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit;

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Deze definitie wordt door de invoering van de Algemene Verordening Gegevensbescherming gewijzigd.

AVG: artikel 4 sub 1 van de Europese Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming, in Engels: GDPR)

'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

LET OP: de AVG bevat in artikel 4 een aantal nieuwe definities die ook betrekking hebben op Persoonsgegevens. Dit zijn de definitie over: Profiling (sub 4), Pseudonimisering (sub 5), Genetische Gegevens (sub 13), Biometrische Gegevens (sub 14). Deze nieuwe definities worden in de AVG verder uitgewerkt in nieuwe artikelen.

Opmerking bij de nieuwe definitie van "Persoonsgegeven"

De nieuwe definitie van Persoonsgegeven zal direct gaan gelden bij het van toepassing worden van de AVG (25 mei 2018). De tekst van de definitie is uitgebreid en meer specifiek omschreven mede als gevolg van de technologische ontwikkelingen waardoor nieuwe mogelijkheden om persoonsgegevens te gebruiken en beschermen zijn ontstaan. De intentie is om een ruimere definitie van persoonsgegeven te bepalen en tegelijkertijd het gebruik van anonimisering en pseudonimisering aan te moedigen. Een en ander blijkt uit de overwegingen 6, 23, 28, 29, 30:

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly.

Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.

(28) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection.

(29) In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure, for the respective processing, that the provisions of this Regulation are implemented, and ensuring that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the data shall also refer to authorised persons within the same controller.

(30) Individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers or other identifiers such as Radio Frequency Identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them.

De Nederlandse tekst van de AVG is geldend in Nederland. Echter, de Engelse tekst leest makkelijker dan de Nederlands/Vlaamse vertaling. Vandaar dat hier de Engelstalige overwegingen zijn weergegeven.

ONDERZOEKEN AP en OPINIE WG-29

In ieder onderzoek van de AP (voorheen CBP) wordt allereerst beoordeeld of sprake is van een "persoonsgegeven". In deze onderzoeken verwijst de AP naar de wetgeschiedenis en ook naar een specifieke opinie van de Artikel 29 Werkgroep. Bij veel gegevens is direct duidelijk dat sprake is van persoonsgegevens, bijvoorbeeld bij naam-adres-woonplaats gegevens. Bij sommige gegevens is het de vraag of indirecte identificatie op zich of in combinatie met andere gegevens (nog) mogelijk is en hoe dit criterium moet worden ingevuld. Vervolgens wordt in de onderzoeken ingegaan of sprake is van een gewoon persoonsgegeven of een "bijzonder persoonsgegeven" (artikel 16 Wbp) waarvoor in principe een verwerkingsverbod geldt.

De AP had altijd al de neiging om het begrip "persoonsgegeven" ruim uit te leggen. In de meest recente onderzoeken lijkt het alsof de AP een nieuw begrip introduceert door bij herhaling de niet wettelijke term "*gevoelige gegevens*" of "*gegevens van gevoelige aard*" te introduceren. Voor dergelijke gegevens gelden in ieder geval extra informatieverplichtingen ex artikel 34 Wbp en zal de meldplicht inzake datalekken sneller van toepassing zijn.

Onderzoeken

- 5 november 2015 (z2015-00409): Onderzoek naar video-opnames van vrachtwagenchauffeurs met de eventrecorder door transportbedrijf De Rooy Transport B.V.

Het CBP zet nogmaals uiteen wanneer beeldgegevens kwalificeren als bijzondere persoonsgegevens. Beeldmateriaal wordt niet als een bijzonder persoonsgegeven in de zin van hoofdstuk 2 van de Wbp aangemerkt als:
- het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven;
- het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid; en
- de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking.
Indien de verwerking van beeldmateriaal echter identificatie tot doel heeft, wordt dit beeldmateriaal wel als een rasgegeven aangemerkt.

- November 2015 (z2014-00859): Onderzoek naar de verwerking van persoonsgegevens in het kader van de Nike+ Running app door Nike Inc.

Het CBP zet vanaf pagina 41 zeer uitvoerig uiteen wanneer sprake is van een persoonsgegeven aan de hand van de Wbp, maar ook aan de hand van het artikel over tracking-cookies (artikel 11.7a lid 4 Telecommunicatiewet), waarin een vermoeden staat dat sprake is van een persoonsgegevens zodra sprake is van verzamelen, analyseren en combineren van gegevens over een gebruiker van randapparatuur (hier een mobiele telefoon waarmee een app wordt gebruikt en een account aangemaakt op een website). Wordt een dergelijk cookie aangetroffen, dan is de Wbp (weerlegbaar) van toepassing.
Het CBP verwijst naar het arrest van het Hof van Justitie van de EU van 24 november 2011 en de conclusie van A-G Jääskinen van 25 juni 2013 om te stellen dat het IP-adres een persoonsgegeven is.
Het CBP stelt dat locatiegegevens persoonsgegevens van gevoelige aard zijn. Vervolgens wordt uitgelegd wat de positie van deze categorie gegevens is in het kader van de Wbp.
Ruime uitleg van gezondheidsgegevens als bijzonder persoonsgegeven: Het (door de tijd heen) meten en vastleggen van activiteiten van mensen waarmee ze hun levensverwachting direct (positief of negatief) beïnvloeden, dient daarom als een verwerking van gezondheidsgegevens te worden gekwalificeerd. Nike registreert door de tijd heen de gegevens over de hardloopactiviteiten, en kan daaraan conclusies verbinden over een levensverwachting, dus verwerkt Nike via de Running app gezondheidsgegevens.
Diverse berekeningen die door Nike worden uitgevoerd met de gegevens verkregen via de app of het account vormen aparte verwerkingen van gezondheidsgegevens.

Ook overweegt het CBP: Het begrip 'gezondheidsgegevens' is veel breder dan het begrip 'medische gegevens'. Het gaat ook niet alleen om gegevens waaruit blijkt dat iemand een slechte gezondheid heeft.

- Oktober 2015 (z2014-00944): Wifi-tracking van mobiele apparaten in en rond winkel door Bluetrace

Opmerkelijk oordeel van CBP: Hoewel Bluetrace de naam van de betrokkene alleen kan achterhalen met aanvullende data, bijvoorbeeld door ten tijde van de detectie van het mac-adres door de sensoren de betrokkene aan te spreken in of bij een winkel, is toch sprake van een persoonsgegeven, want het is niet cruciaal voor de definitie van persoonsgegevens of een verantwoordelijke de naam van een betrokkene kan achterhalen. Bluetrace heeft aangevoerd dat sprake is van een zuiver theoretische mogelijkheid om de betrokkene te identificeren, maar CBP stelt dat: Niet *iedere* mogelijkheid om de gegevens voor de herleiding van personen te gebruiken moet zijn uitgesloten, om te mogen concluderen dat er geen sprake is van persoonsgegevens. Indien de mogelijkheid theoretisch aanwezig is, maar het ondenkbaar is dat dit daadwerkelijk gebeurt, kan men ervan uit gaan dat de gegevens niet als persoonsgegeven worden aangemerkt (dit volgt uit de MvT bij de Wbp). In casu, oordeelde het CBP dat tóch sprake was van een persoonsgegeven, zie hierna bij de weergave.
Ook geeft het CBP een overweging over het feit dat de locatiegegevens van een mobiele telefoon in principe overeenkomen met de locatiegegevens van de eigenaar, dus dat al snel sprake is van een set van gegevens die is zeggen over een persoon. Dit lijkt een verwijzing naar overweging 30 van de AVG, waarvan de tekst ten tijde van dit Bluetrace onderzoek nog onderwerp van Europees overleg was.
Ook merkt het CBP op dat hashing alleen als dit onomkeerbaar is, leidt tot anonimisering. Hashing is naar haar aard niet bedoeld om gegevens te anonimiseren. Ook wordt ingegaan op pseudonimisering en anonimisering.

- April 2015 (z2014-00135): Onderzoek naar de verwerking van persoonsgegevens met betrekking tot of door het gebruik van interactieve digitale televisiediensten van Ziggo

Gegevens over kijkgedrag zijn persoonsgegevens van gevoelige aard: Omdat het hierbij over inhoudelijke gegevens gaat over het kijkgedrag, zijn het persoonsgegevens van gevoelige aard. De kwalificatie 'persoonsgegevens van gevoelige aard' zegt iets over de impact die de verwerking van het betreffende gegeven kan hebben op de persoonlijke levenssfeer van de betrokkene in een bepaalde situatie. Het CBP merkt gegevens over kijkgedrag aan als gevoelige gegevens omdat het verzamelen van dergelijke gegevens kan leiden tot een indringend beeld van iemands persoonlijke voorkeuren en levensovertuigingen. Dit geldt in het bijzonder voor gegevens over het kijkgedrag naar erotische films en zenders.

- Juli 2013 (z2012-00605): Onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart tv door TP Vision Netherlands B.V.

Philips smart tv. Vanaf p. 50 een uitvoerige analyse, waarbij ook wordt ingegaan op de zienswijze van Philips en TP Vision, van de vraag wanneer bepaalde (technische) gegevens of combinatie van gegevens kwalificeren als persoonsgegevens.
Het Device ID, Consumer ID en Mobile Device ID met de naam van het mobiele apparaat (unieke klant- of toestel-identifiers), in onderlinge combinatie of in samenhang met gegevens over het onlinekijk- en internetgedrag (bekeken uitzendingen, gehuurde films, bezoek aan en gebruik door een betrokkene van apps en websites, tijdstippen van aan- en uitzetten van het toestel) zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon. De persoonsgegevens over het onlinekijkgedrag van betrokkenen zijn bovendien gegevens van gevoelige aard, omdat zij veel over personen zeggen. Gevolgd door een uitleg wat “gegevens van gevoelige aard” zijn.

Niet doorslaggevend is of TP Vision de bedoeling heeft om de individuele betrokkenen te benaderen voor (direct) marketing- en profileringsdoeleinden. Er is al sprake van een persoonsgegeven wanneer het gegeven voor een op de persoon gericht doel kan worden gebruikt, en die mogelijkheid is aanwezig.

TP Vision beschikt (in ieder geval via de IP-EPG-logbestanden) over de IP-adressen waarmee de smart tv aan internet is verbonden. Bij de internetserviceprovider zijn de IP-adressen gekoppeld aan NAW-gegevens. Deze NAW-gegevens kunnen via een gerechtelijk bevel aan TP Vision of bijvoorbeeld aan opsporingsinstanties verstrekt worden. De IP-adressen zijn daarom herleidbaar naar identificeerbare natuurlijke personen.

Het CBP wijst op het feit dat de definitie van persoonsgegevens niet alleen herleidbaarheid omvat door de verantwoordelijke zelf, maar ook door een derde. Omdat ISP's de IP-adressen kunnen herleiden naar natuurlijke personen, is er de facto sprake van identificeerbare gegevens, en omdat de gegevens ook door de politie opgevraagd kunnen worden ten behoeve van de opsporing, dienen ze als persoonsgegevens te worden beschouwd. Het gaat bij TP Vision bovendien niet over een verzameling losse IP-adressen op zichzelf, maar om gegevens in onderlinge combinatie of in samenhang met gegevens over individueel kijkgedrag, websitebezoek en appgebruik die direct dan wel indirect −redelijkerwijs, zonder onevenredige inspanning − herleidbaar zijn tot een identificeerbare natuurlijke persoon. De stelling dat het bij IP-adressen om gecodeerde gegevens zou gaan, kan het CBP evenmin onderschrijven. Het gaat hier niet om gegevens die door of in opdracht van een verantwoordelijke zijn ontdaan van identificerende gegevens dan wel versleuteld, en al evenmin om bescherming tegen ontsleuteling via een beroepsgeheim.

Ook volgt een uitgebreide analyse van het begrip tracking cookies en gebruikmaking van Google Analytics.

Contractuele mogelijkheden spelen een rol bij de bepaling of sprake is van persoonsgegevens:

Hoewel TP Vision heeft verklaard geen registratiegegevens te ontvangen van Philips en dit ook is bepaald in de licentieovereenkomst tussen TP Vision en Philips (zie p. 28 van dit rapport), kan TP Vision wel degelijk inzage krijgen in de NAW-gegevens die horen bij het Consumer ID (en bij Philips berusten), met een beroep op de marketingclausule in de overeenkomst met Philips. Het feit dat Philips deze inzage tot op heden niet heeft verleend, zoals TP Vision schrijft, laat onverlet dat de contractuele mogelijkheid bestaat. Ook zou TP Vision via een rechterlijke procedure afgifte door Philips kunnen afdwingen van de NAW-gegevens behorend bij een of meerdere Consumer ID's, bijvoorbeeld in het (hypothetische) geval dat TP Vision aansprakelijk gesteld zou worden voor een auteursrechtinbreuk door een of meerdere gebruikers van Philips smart tv's.

Het Consumer ID is een zelfstandig persoonsgegeven omdat het voor Philips (bij alle geregistreerde klanten) rechtstreeks herleidbaar is naar geïdentificeerde natuurlijke personen. Het feit dat TP Vision het systeem zodanig heeft opgezet dat de registratiegegevens bij Philips berusten en dat de gegevens over het kijkgedrag in beginsel gescheiden worden gehouden van de registratiegegevens, leidt niet tot de conclusie dat er geen sprake is van persoonsgegevens.

Identificatie kan ook plaatsvinden zonder dat de naam van de betrokkene wordt achterhaald, zoals ook WP29 toelicht in zijn advies over persoonsgegevens. Vereist is slechts dat de betrokkene aan de hand van de beschikbare informatie in combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) van andere personen kan worden onderscheiden.

Ook de doeleinden van de verwerking kunnen bepalen dat sprake is van een persoonsgegeven:

De gegevensverwerking is (dan) mede gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens, conform het advies over persoonsgegevens van de Artikel 29-werkgroep.

Dat een object door meerdere mensen kan worden gebruikt, maakt nog niet dat geen sprake is van een persoonsgegeven:

Dat een televisie door meerdere personen in een huishouden kan worden gebruikt, laat onverlet dat het wel degelijk om persoonsgegevens gaat. Een vaste telefoon kan ook door meerdere personen in het huishouden worden gebruikt. Dit geldt ook voor bijvoorbeeld een auto. Dit staat, ook volgens de parlementaire geschiedenis van de Wbp, niet in de weg aan de conclusie dat het een persoonsgegeven betreft als de gegevens over het gebruik aan de houder van de telefoon of auto worden toegerekend.

Ten aanzien van het door TP Vision genoemde voorbeeld van het studentenhuis acht het CBP herleidbaarheid overigens ook mogelijk. Als een van de studenten via video on demand bijvoorbeeld een film bestelt, zal dat op de eindafrekening zichtbaar worden, en zal degene die de facto de rekening betaalt, de werkelijke kijker kunnen en willen identificeren.

- 11 juni 2013 (Z2011-00462): Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door T-Mobile Netherlands B.V.

Zeer uitvoerige analyse van verschillende soorten (technische) gegevens die kunnen kwalificeren als persoonsgegevens.
Gegevens 'betreffende' een persoon: Het MSISDN, IMSI-klantnummer en het IMEI-toestelnummer (unieke klant- of toestel identifiers), op zichzelf of in onderlinge combinatie of in samenhang met (technische) gegevens over het bezoek aan en gebruik door een betrokkene van apps, websites en protocollen zijn naar hun aard gegevens over gedragingen van een natuurlijke persoon (informatie over zijn mobiele data ge-/verbruik). Datzelfde geldt voor de locatiegegevens, die een beeld kunnen geven van de verplaatsingen van de betrokkene, met tijd. Daarnaast zijn unieke klant- en/of toestel identifier(s), in combinatie met (technische) gegevens over het functioneren van het netwerk/toestel bij het gebruik daarvan door een individuele betrokkene gegevens over een natuurlijke persoon. T-Mobile kan deze gegevens aanwenden om de betrokkene op een bepaalde wijze te behandelen of het gedrag van die persoon te beïnvloeden, op een wij ze die gevolgen heeft voor de rechten/belangen van de betrokkene. Daarbij valt bijvoorbeeld te denken aan het analyseren van de inhoud van (gedownloade) bestanden en verzonden en ontvangen e-mails op virus- en malware-herkenningspatronen om virussen/malware tegen te houden en te verwijderen of aan het analyseren van het dataverkeer om een verzoek om inlichtingen af te handelen (oftewel, het gebruik van de gegevens in individuele gevallen met betrekking tot abonnees om technische defecten of fouten in de overbrenging van communicatie op te sporen en te verhelpen). De gegevens worden dus door T-Mobile gebruikt op een wijze die in het maatschappelijk verkeer de betrokkene raakt.
Verder kan het mobiele data ge-/verbruik van een betrokkene een indicatie zijn voor bijvoorbeeld zijn interesses, sociale achtergrond, inkomen of gezinssamenstelling. Dergelijke informatie kan worden gebruikt voor (direct) marketing- en profileringsdoeleinden. Niet doorslaggevend is of T-Mobile de bedoeling heeft om de gegevens over en uit het dataverkeer of voor die doeleinden of andere doeleinden te gebruiken. Er is al sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel kan worden gebruikt, en die mogelijkheid is aanwezig.
Identificeerbaarheid van de persoon: De gegevens over en uit het dataverkeer zijn op zichzelf, in onderlinge combinatie of in samenhang met uit andere bron bekende informatie voor T-Mobile direct dan wel indirect herleidbaar tot een identificeerbare natuurlijke persoon (abonnee van haar dataverkeersdiensten).

En, het toepassen van technische en organisatorische maatregelen is enkel voldoen aan artikel 13 Wbp, dit maakt niet dat geen sprake is van persoonsgegevens:
De omstandigheid dat slechts bepaalde medewerkers toegang hebben tot de data-analyse apparatuur en de data die met behulp daarvan wordt verwerkt, leidt echter niet tot de conclusie dat er geen sprake is van persoonsgegevens. De toegepaste aggregatie op abonnee-niveau is geen anonimisering of gegevensvernietiging. De [VERTROUWELIJK] bevatten nog [VERTROUWELIJK] het e-mailadres van de T-Mobile abonnee die met een e-mailaccount van een (andere) provider mailt of een derde die een T-Mobile klant mailt).

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

verondersteld dat de voor de verwerking verantwoordelijke over "redelijkerwijs in te zetten middelen" beschikt om de betrokkene te identificeren. Aan te voeren dat personen niet identificeerbaar zijn als het doel van de verwerking nu juist die identificatie is, komt neer op een contradictio in terminis. De informatie moet dan ook worden beschouwd als informatie betreffende identificeerbare personen, wat betekent dat voor de verwerking de regels inzake gegevensbescherming gelden." Dit is volgens de opinie van de Artikel 29 Werkgroep met name relevant voor statistische informatie, wanneer de informatie weliswaar wordt gepresenteerd als geaggregeerde gegevens, maar (de) andere gegevens identificatie van betrokkenen mogelijk maken. Om de hiervoor genoemde doeleinden (i) tot en met (iii) te verwezenlijken moeten de verwerkte gegevens herleidbaar zijn tot de betrokken abonnees. De gegevensverwerking is (dan) mede gericht op identificatie, zodat de gegevens dienen te worden aangemerkt als persoonsgegevens.

Vervolgens volgt een analyse van wanneer verkeersgegevens en communicatiegegevens als persoonsgegevens kunnen kwalificeren:
De gegevens over het dataverkeer zijn (derhalve) zulke verkeersgegevens (die ook persoonsgegevens zijn), voor zover er daadwerkelijke communicatie plaatsvindt. De verkeersgegevens over het communicatiegedrag van betrokkenen (bijvoorbeeld URL's) zijn gegevens van gevoelige aard.

Samengevat, kunnen de persoonsgegevens worden ingedeeld in twee categorieën:

1. persoonsgegevens die ook verkeersgegevens zijn, namelijk gegevens over het dataverkeer zoals unieke klant- en toestel identifiers (bijvoorbeeld het 06- nummer), de starttijd en eindtijd van de data sessie, verbruikte datavolume, IP-adres van-naar met poortnummer/protocol, URL's, locatiegegevens etc.
2. persoonsgegevens die ook communicatie betreffen (en dus geen verkeersgegevens), namelijk virus- en malwareherkenningsgegevens uit de inhoud van het dataverkeer.

- Diverse packet inspection onderzoeken, waaronder
  20 juni 2013 (z2011-00462): Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Vodafone Libertel B.V.

Gelijk als in het T-mobile onderzoek van 11 juni 2013 (Z2011-00462) een uitvoerige analyse wanneer mobiele data als persoonsgegeven kwalificeert. Daarnaast blijkt dat het beschikbare personeel bij een verantwoordelijke ook een bepalende rol speelt bij de vraag of sprake is van herleidbaarheid naar een natuurlijke persoon:
Niet alleen beschikt Vodafone over de (in)direct identificerende gegevens over en uit het dataverkeer in haar databases/bestanden, ook heeft zij ter zake kundige technici in dienst (waaronder de eerder genoemde medewerkers; zie het kopje 'Verloop onderzoek', p. 10 e.v. van dit rapport) en beschikt zij over de benodigde technische faciliteiten (waaronder applicaties om de databases te bevragen en de technische mogelijkheid om gegevens te exporteren uit deze databases) om de gegevens aan elkaar te koppelen of zo nodig via tussenstappen te herleiden naar de betrokken abonnee. Hieruit blijkt dat de inspanning die Vodafone moet verrichten om deze gegevens naar een individuele natuurlijke persoon te (kunnen) herleiden niet onevenredig is.
Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen (mere conduit), verwerkt daarmee geen persoonsgegevens.

- 7 december 2010 (z2010-00582): Onderzoek naar de verzameling van Wifigegevens met Street View auto's door Google z2010-00582:

De verzamelde MAC-adressen van wifi-routers, in combinatie met de berekende locatie, zijn in deze context persoonsgegevens in de zin van artikel 1, onder a, Wbp omdat het uniek identificerende nummers zijn waarmee individuele houders geïdentificeerd kunnen worden.

Het CBP heeft in eerder onderzoek eveneens vastgesteld dat het genereren en gebruiken van de combinatie van (a) mac-adressen en (b) de berekende locatie van een wifi-router aan te merken is als een verwerking van gegevens over identificeerbare personen.

Opinie WG-29

In 2007 heeft de WG29 een opinie specifiek over het begrip Persoonsgegeven gepubliceerd. Daarnaast heeft de WG zich in verschillende opinies uitgelaten over het begrip Persoonsgegeven met betrekking tot verschillende contexten.

Specifiek over Persoonsgegeven:
WP29 (136) Opinie 4/2007 on the concept of personal data, 20 juni 2007
Vindplaats: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

In dit kader ook interessant:

- WP 29 (223) Opinie 8/2014 on the on Recent Developments on the Internet of Things, 16 september 2014

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

> Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.
> For instance, wearable things kept in close proximity of data subjects result in the availability of a range of other identifiers, such as the MAC addresses of other devices which could be useful to generate a fingerprint allowing data subject location tracking. The collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals. These fingerprints and identifiers could be used for a range of purposes, including location analytics or the analysis of movement patterns of crowds and individuals.
> Such a trend must be combined with the fact that such data can later be combined with other data issued from other systems (e.g. CCTV or internet logs).
>
> In the context of the IoT, it is often the case that an individual can be identified based on data that originates from “things”. Indeed, such data may allow discerning the life pattern of a specific individual or family – e.g. data generated by the centralised control of lighting, heating, ventilation and air conditioning.
> Furthermore, even data relating to individuals that is intended to be processed only after the implementation of pseudonymisation, or even of anonymisation techniques may have to be considered as personal data. In fact, the large amount of data processed automatically in the context of IoT entails risks of re-identification. On this point, the Working Party refers to the relevant developments described in its recent opinion on anonymisation techniques, which helps identifying these risks and makes recommendations as to the implementation of these techniques.

- WP 29 (216) Opinie 5/2014 over anonimiseringstechnieken, april 2014

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- WP 29 (202) Opinie 02/2013 on apps on smart devices, d.d. 27 februari 2013

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

- WP 29 (193) Opinion 3/2012 on developments in biometric technologies, 27 april 2012

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

- WP 29 (185) Opinie 13/2011 on Geolocation services on smart mobile devices adopted, d.d. 16 mei 2011

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp185_en.pdf

- WP 29 (160) Opinie 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 februari 2009

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

- WP 29 (147) Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), 18 februari 2008

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf

- WP29 (115) Opinie on the use of location data with a view to providing value added services, November 2005

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

- WP 29 (105) Working document on the data protection issues related to RFID technology, 19 januari 2005

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

- WP 29 (111) Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, 28 september 2005

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp111_en.pdf

- WP 29 (48) Opinie 8/2001 on the processing of personal data in the employment context, 13 september 2001

Vindplaats: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

WEERGAVE VAN INVULLING VAN HET BEGRIP PERSOONSGEGEVEN DOOR AP

In de openbare versie van de onderzoeken van de AP (CBP) wordt gewerkt met tekstblokken. Het is dus raadzaam om bepaalde overwegingen uit onderzoeken van de AP bij het bepalen of sprake is van een "Persoonsgegeven" door te lezen. Houdt u wel rekening met alle mogelijke vormen van invulling van de overwegingen (tekstblokken) door de AP aan de hand van de feiten en omstandigheden van uw specifieke casus. Indien van toepassing: ga in uw zienswijze specifiek in op de feiten en omstandigheden die in uw geval bepalen dat geen sprake is van een "Persoonsgegeven".

LET OP: Gezien de tendens in de Opinies van de WG 29, de nieuwe definitie in de AVG van het begrip Persoonsgegeven en de sterke neiging van de AP om te oordelen dat altijd sprake is van een Persoonsgegeven, is het heel lastig om met succes te stellen dat géén sprake is van een Persoonsgegeven.

<u>In het onderzoek bij Bluetrace d.d. 13 oktober 2015 (vanaf pagina 23):</u>

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

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp en omvat onder meer het verzamelen, vastleggen, bewaren, gebruiken, samenbrengen en met elkaar in verband brengen van persoonsgegevens.

Artikel 1, aanhef en onder a, van de Wbp vormt een implementatie van artikel 2, aanhef en onder a, van de Europese Privacyrichtlijn:

"*In de zin van deze richtlijn wordt verstaan onder (…) 'persoonsgegevens', iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.*"

Overweging 26 van de Privacyrichtlijn luidt in dit verband:

"*Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is (…).*"

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd. Het CBP verwijst in dit verband ook naar de adviezen 5/2014 (over anonimiseringsmethoden) en 13/2011 (over geolocatiefuncties op mobiele apparaten) van de Artikel 29 werkgroep, het samenwerkingsverband van Europese toezichthouders op basis van artikel 29 van de ePrivacy Richtlijn. In de laatstgenoemde opinie zijn locatiegegevens (van mobiele telefoons) door de Europese privacytoezichthouders aangemerkt als persoonsgegevens van gevoelige aard: "*Omdat smartphones en tabletcomputers onlosmakelijk verbonden zijn met hun eigenaren, leveren de verplaatsingen van de apparaten een zeer intieme inkijk in het leven van hun eigenaren.*"

Dit kader wordt in het hoofdstuk Beoordeling (5) van het onderzoek op geheel eigen wijze door het CBP ingevuld (vanaf pagina 30):

5.1 Verwerking van persoonsgegevens

Het CBP heeft in paragraaf 3.4 van dit rapport vastgesteld dat Bluetrace ten minste de onderstaande gegevens genereert en verzamelt (en heeft verzameld) met wifitracking.

- Het mac-adres van mobiele apparaten, met name telefoons;
- De signaalsterkte van het geregistreerde wifi- signaal van de apparaten;
- Het serienummer van de sensor;
- Het tijdstip van de meting.

Op basis van deze vier kenmerken verricht Bluetrace wifi-tracking in winkels en wifitracking buiten winkels op de openbare weg Het gebruik van deze combinatie van gegevens is een verwerking van persoonsgegevens, omdat daarmee individuele betrokkenen, namelijk houders van de betreffende apparaten, identificeerbaar zijn.

Volgens artikel 1, aanhef en onder a, Wbp wordt onder een persoonsgegeven verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Gegevens moeten geschikt zijn om een persoon te identificeren of althans direct of indirect identificeerbaar zijn om te kunnen spreken van persoonsgegevens.

Direct identificerende gegevens

Van direct identificerende gegevens is in dit geval geen sprake. Het gaat hier niet om gegevens als namen, adressen en telefoonnummers. Er bestaat ook geen opzoektabel van mac-adressen en het eigendom van de betreffende apparatuur.

Indirect identificerende gegevens

Er kan wel sprake zijn van indirect identificeerbare gegevens, indien gegevens, zonder dat zij namen bevatten, door combinatie met elkaar of met andere gegevens teruggebracht kunnen worden tot een bepaalde persoon. Een persoon is identificeerbaar indien zijn identiteit – direct of via nadere stappen, door gegevens die alleen of in combinatie met andere gegevens zo kenmerkend zijn voor zijn persoon – redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Er moet worden uitgegaan van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise en technische faciliteiten van de verantwoordelijke.

In de Wbp is rekening gehouden met de voortdurende innovatie in de informatietechnologie: "*Bij het voortschrijden van informatietechnologie moet rekening worden gehouden met het feit dat waar voorheen wellicht nog sprake was van een onevenredige inspanning (en dus niet van een persoonsgegeven), deze inspanning geringer wordt met het beschikbaar komen van nieuwe technieken. Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.*"

Identificatie zonder naam

Identificatie kan ook plaatsvinden zonder dat de naam van de persoon wordt achterhaald. Vereist is slechts dat de gegevens ervoor zorgen dat een bepaald persoon kan worden onderscheiden van anderen. In de opinie van de Artikel 29-werkgroep over het begrip persoonsgegeven is hierover opgemerkt: *"(…) dat hoewel*

identificatie door middel van de naam in de praktijk het meest voorkomt, de naam niet in alle gevallen noodzakelijk is om een persoon te identificeren. Dit is het geval wanneer andere identificatiemiddelen worden gebruikt om iemand van anderen te onderscheiden. In computerbestanden waarin persoonsgegevens zijn opgenomen, wordt aan de geregistreerde personen doorgaans een unieke identificatiecode toegewezen om verwisseling van personen in het bestand te voorkomen. Op het world wide web is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook van de gebruiker ervan. (…) Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van 'persoonsgegeven' weerspiegelt ook dit feit." [onderstrepingen toegevoegd door het CBP].
Als de gegevens niet direct tot identificatie van een bepaald persoon leiden maar de gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon, betreft het indirect identificerende persoonsgegevens. De memorie van toelichting van de Wbp schrijft hierover: "*Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.*

Identificatie door combinatie van objectgegevens en andere gegevens
De memorie van toelichting bij de Wbp beschrijft dat als persoonsgegevens worden beschouwd "alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon". Ook gegevens die niet direct betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen soms informatie verschaffen over een bepaalde persoon, bijvoorbeeld wanneer daarmee de arbeidsproductiviteit van een werknemer gemakkelijk in kaart kan worden gebracht.
In dit verband is het van belang om persoonsgegevens te onderscheiden van "objectgegevens". De wetsgeschiedenis schrijft hier over: "*Gegevens die uitsluitend voorwerpen aanduiden, (…) zijn geen persoonsgegevens indien deze geen informatie bevatten met behulp waarvan personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere objectgegevens.*" Wanneer een objectgegeven wordt gecombineerd met andere informatie kan er een set gegevens ontstaan die informatie betreffende een persoon kan verschaffen.

Locatiegegevens
Locatiegegevens (van mobiele telefoons) zijn door de Europese privacytoezichthouders aangemerkt als persoonsgegevens van gevoelige aard: "*Omdat smartphones en tabletcomputers onlosmakelijk verbonden zijn met hun eigenaren, leveren de verplaatsingen van de apparaten een zeer intieme inkijk in het leven van hun eigenaren*."

Identificeerbaarheid meetgegevens wifi-tracking van Bluetrace
Hoewel Bluetrace de naam van de betrokkene alleen kan achterhalen met aanvullende data, bijvoorbeeld door ten tijde van de detectie van het mac-adres door de sensoren de betrokkene aan te spreken in of bij een winkel, is het niet cruciaal voor de definitie van persoonsgegevens of een verantwoordelijke de naam van een betrokkene kan achterhalen

Het mac-adres van een mobiel apparaat is een identificerend kenmerk van dat apparaat, in die zin dat het mobiele apparaat altijd hetzelfde mac-adres uitzendt en de aanwezigheid van een apparaat in de buurt van een sensor vergeleken kan worden met eerder opgeslagen waarnemingen van dat mac-adres en met het mac-adres in het apparaat zelf. (bijvoorbeeld de mobiele telefoon)

Het zijn feiten van algemene bekendheid dat smartphones zeer persoonlijke apparaten zijn, dat zij zelden gedeeld worden met meerdere personen en dat de locatie van een telefoon gedurende het grootste gedeelte van een dag overeenkomt met de verblijfplaats van de eigenaar. Het CBP gaat er daarom van uit dat de exacte locatie van een smartphone in onze huidige maatschappij onmiskenbaar informatie over de verblijfplaats van diens eigenaar geeft. Bluetrace combineert een objectgegeven (macadres) met aanvullende informatie over de datum, het tijdstip en de plaats waar het mac-adres is waargenomen. Daarbij is van belang dat mac-adressen unieke apparaten onderscheiden en dat die apparaten, in de context van geolocatiediensten, rechtstreeks verbonden zijn met de locatie van een houder. Daarmee is er sprake van een set gegevens die informatie kan verschaffen over een persoon.

Bluetrace heeft er tijdens het onderzoek meerdere malen op gewezen dat het bedrijf ervan uitgaat dat herleidbaarheid van meetgegevens uit wifi-tracking naar personen een zuiver theoretische mogelijkheid is. Bluetrace stelt onder andere dat deze gegevens voor het bedrijf redelijkerwijs niet herleidbaar zijn naar individuele personen. Om deze reden gaat Bluetrace ervan uit dat het bedrijf geen persoonsgegevens verwerkt. Bluetrace heeft daarnaast verklaard dat identificatie van personen ook niet het doel is van de gegevensverwerkingen.

Niet iedere mogelijkheid om de gegevens voor de herleiding van personen te gebruiken moet zijn uitgesloten, om te mogen concluderen dat er geen sprake is van persoonsgegevens. De memorie van toelichting bij de Wbp geeft aan dat wanneer deze mogelijkheid weliswaar theoretisch aanwezig is, maar het ondenkbaar is dat dit ook daadwerkelijk gebeurt, men ervan uit kan gaan dat de gegevens niet als persoonsgegevens worden aangemerkt. De memorie van toelichting bij de Wbp bepaalt in dit verband echter ook dat: "*uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening gehouden worden met de bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke*."

Het CBP acht van belang dat Bluetrace zelf de sensoren installeert ter plaatse. Bluetrace weet dus exact welke sensor op welke fysieke locatie staat. De combinatie van het sensornummer met de gegevens over de signaalsterkte maakt het voor Bluetrace eenvoudig om de locatie van het geregistreerde apparaat vast te stellen. Wanneer er een aantal mac-adressen geregistreerd wordt op een bepaalde plek en op een bepaald tijdstip, dan is tegelijkertijd ook fysiek waar te nemen welke mensen daar op dat moment lopen. Dit kan door een mens, bijvoorbeeld een medewerker van Bluetrace of van een winkel, op de locatie waargenomen worden. De betrokkene kan op dat moment persoonlijk benaderd worden.

De herleidbaarheid naar personen is geen strikt theoretische mogelijkheid. Zoals toegelicht in paragraaf 3.2 van dit rapport, heeft Bluetrace tijdens het onderzoek van het CBP verklaard dat het voor is gekomen dat de politie meetgegevens heeft opgevraagd bij Bluetrace voor opsporingsonderzoeken. Het is ook voorgekomen dat een klant van Bluetrace gegevens heeft opgevraagd in verband met winkeldiefstal, om de dader op te kunnen sporen.

De wetgever merkt in de memorie van toelichting bij de Wbp expliciet op: "*Indien het (…) mogelijk is de gegevens te gebruiken om fraude op te sporen, dan is sprake van een persoonsgegeven. Daarbij is niet relevant of de bedoeling om de gegevens voor dat doel te gebruiken ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt.*"

Zowel uit de praktijk bij Bluetrace als uit recente rechtspraak is duidelijk geworden dat de gegevens zich lenen voor toepassing van een dergelijk op de persoon gericht doel. Het CBP verwijst naar een uitspraak van het Gerechtshof Arnhem-Leeuwarden van 27 november 2014. Deze uitspraak heeft betrekking op een strafzaak waarin tijdens het opsporingsonderzoek naar strafbare feiten gebruik gemaakt is van de meetgegevens van bluetooth-trackinginstallaties van de Verkeersinformatiedienst, om te bewijzen dat de verdachte aanwezig was op bepaalde plaatsen. Mede op basis van de beschikbare gegevens over tracking van mobiele apparatuur, zoals telefoons, kon geconcludeerd worden dat de verdachte medeplichtig was aan moord. Omdat het mac-adres van de telefoon van de verdachte bekend was bij de opsporingsdiensten, was eenvoudig te achterhalen waar zijn telefoon zich bevond omstreeks het tijdstip waarop het delict was gepleegd. De rechter heeft dit gebruikt als bewijsmiddel omtrent de verblijfplaats van deze persoon.

In de jurisprudentie komen daarnaast andere gevallen voor waarin sprake is van het achterhalen van een persoon die een apparaat gebruikt en/of het achterhalen van diens verblijfplaats aan de hand van het mac-adres van een telefoon, een wifi-router, een simkaart of een laptop. Mac-adressen met aanvullende meetgegevens worden dus in de praktijk opgevraagd en toegepast om individuele personen – zoals daders of getuigen van strafbare feiten – op te sporen.

Het CBP heeft in eerder onderzoek eveneens vastgesteld dat het genereren en gebruiken van de combinatie van (a) mac-adressen en (b) de berekende locatie van een wifi-router aan te merken is als een verwerking van gegevens over identificeerbare personen.

<u>In onderzoek Nike+ running app d.d. november 2015, p. 45-46</u>

Locatiegegevens; persoonsgegevens van gevoelige aard
Locatiegegevens zijn persoonsgegevens van gevoelige aard, omdat het gegevens zijn die een zeer gedetailleerd beeld kunnen geven van iemands gedrag en belangstelling. De kwalificatie 'persoonsgegevens van gevoelige aard' zegt iets over de impact die het gegeven kan hebben. Deze categorie hoeft dus niet samen te vallen met de categorie *bijzondere persoonsgegevens*, als bedoeld in artikel 16 van de Wbp.

In de wetsgeschiedenis bij artikel 9 Wbp worden de begrippen ‘bijzondere’ en ‘gevoelige’ gegevens als volgt uitgelegd:

“*Artikel 16 betreft de gegevens die uit hun aard gevoelig zijn. Daarnaast kunnen gegevens gevoelig zijn door de context waarin zij worden gebruikt, bij voorbeeld de gegevens omtrent iemands kredietwaardigheid of welstand.”*

De Artikel 29-werkgroep schrijft over locatiegegevens: "*Een slim mobiel apparaat is zeer nauw verbonden met een specifieke persoon. De meeste mensen zijn geneigd om hun mobiele apparaten dicht bij zich te houden, zoals in een broek- of jaszak, in een tas of op het nachtkastje naast het bed. Het gebeurt zelden dat iemand een dergelijk apparaat aan een ander uitleent. (...) Hierdoor kunnen aanbieders van geolocatiediensten een gedetailleerd overzicht van de gewoonten en patronen van de eigenaar van het apparaat verkrijgen en uitgebreide profielen opstellen. Zo kan uit een patroon van inactiviteit in de nacht de slaapplaats worden afgeleid en uit een regelmatig reispatroon in de ochtend de locatie van de werkgever. Het patroon kan ook gegevens omvatten die zijn afgeleid uit bewegingspatronen van vrienden, op basis van zogeheten ‘social graphs’.*" (Opinie WP 185, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, 16 mei 2011, p. 7-8).

<u>En p. 110, inzake de invulling van de informatieplicht ex artikel 34 Wbp:</u>

Ten aanzien van de <u>aard</u> van de gegevens onderstreept het CBP dat Nike bijzondere persoonsgegevens verwerkt, namelijk gezondheidsgegevens, en overige gegevens van gevoelige aard, zoals de locatie van de betrokkenen. Omdat Nike het gebruik van de locatie en gezondheidsgegevens onvoldoende afbakent of toelicht, kan een gemiddelde internetgebruiker de aard en omvang van de gegevensverwerking niet bepalen.

TIPS & TRICKS

- Bij de kwalificatievraag of sprake is van persoonsgegeven dient systematisch te worden gewerkt. De definitie van persoonsgegeven bestaat uit meerdere elementen. Ieder element moet aanwezig zijn. “Informatie”, “betreffende”, “natuurlijke persoon”, “geïdentificeerd” of “identificeerbaar”,
- Let goed op hetgeen staat omschreven in overweging 29 van de Richtlijn en straks overweging 26 van de AVG. Hier staat bij de uitleg van identificeerbaar dat het gaat om identificeerbaar door de verantwoordelijke *of door een andere persoon.* Daar waar het Cbp zich eerst in diverse uitingen beperkte tot identificeerbaar door de verantwoordelijke (een kenteken is niet voor iedereen een persoonsgegeven), zo lijkt met het Bluetrace onderzoek een aanzet te zijn gegeven voor een ruimere uitleg door ook de andere persoon (politie en justitie) te betrekken bij de identificeerbaarheid. Bij Bluetrace bleek dit bedrijf overigens zelf ook tot identificatie in staat te zijn;
- Een set gegevens die afzonderlijk niet tot een persoon te herleiden zijn, kunnen gezamenlijk toch ervoor zorgen dat sprake is van persoonsgegevens;
- Indien het doel van de verwerking is gericht op identificatie, is daardoor de kwalificatie als persoonsgegeven al mogelijk;
- Indien gegevens kunnen worden gebruikt om fraude tegen te gaan, dan is sprake van een persoonsgegeven;
- Locatiegegevens zijn persoonsgegevens van gevoelige aard, waarbij dus een extra informatieplicht geldt;
- Een pasfoto is een bijzonder persoonsgegeven omtrent ras in de zin van artikel 16 en 18 Wbp;
- Gegevens over kijkgedrag of surfgedrag zijn gegevens van gevoelige aard;
- Het bijzondere persoonsgegeven, gezondheidsgegeven, wordt ruim uitgelegd. Ieder gegeven dat betrekking heeft op gezondheid (positief of negatief) is een gezondheidsgegeven;
- Ook al bestaat bij een gegeven of set gegevens de mogelijkheid tot herleiding van een natuurlijke persoon enkel via een gerechtelijk bevel of door tussenkomst van de politie, dan toch sprake van een persoonsgegeven;
- Indien enkel via een contractuele bepaling andere gegevens kunnen worden verkregen waardoor er een combinatie van gegevens ontstaat die wél kwalificeren als persoonsgegeven, dan is toch sprake van de verwerking van persoonsgegevens;
- De enkele aanwezigheid van het gebruik van de gegevens voor marketing- of profileringsdoeleinden, ook al wordt dit niet daadwerkelijk gedaan, maakt dat sprake is van persoonsgegevens;
- Een vaste overweging in de onderzoeken van het CBP/AP is: Ook gegevens die niet betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een product of een proces, kunnen soms informatie verschaffen over een bepaalde persoon. In de memorie van toelichting worden in dit verband telefoonnummers, kentekens van auto’s en postcodes met huisnummers genoemd;
- Naar de huidige stand der techniek kan er bijna vanuit worden gegaan dat géén sprake meer is van de van onevenredige inspanningen om de gegevens tot een natuurlijk persoon te herleiden, waardoor bijna altijd sprake is van een persoonsgegeven.