GROEP GEGEVENSBESCHERMING ARTIKEL 29

01248/07/NL
WP 136

Advies 4/2007 over het begrip persoonsgegeven

Goedgekeurd op 20 juni 2007

Deze groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Civiel recht, grondrechten en burgerschap) van het directoraat-generaal Justitie, vrijheid en veiligheid van de Europese Commissie, B-1049 Brussel, België, kamer LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

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[1],

Gelet op artikel 29 en artikel 30, lid 1, onder a), en lid 3, van die richtlijn en artikel 15, lid 3, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002,

Gelet op artikel 255 van het Verdrag tot oprichting van de Europese Gemeenschap en op Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie,

Gelet op het reglement van orde van de Groep,

HEEFT HET VOLGENDE ADVIES GOEDGEKEURD:

[1] Publicatieblad van de Europese Unie L 281 van 23.11.1995, blz. 31, te vinden op: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

I. INLEIDING 3

II. ALGEMENE OVERWEGINGEN EN BELEIDSVRAGEN 4

III. ANALYSE VAN DE DEFINITIE VAN PERSOONSGEGEVEN IN DE RICHTLIJN GEGEVENSBESCHERMING 6

1. EERSTE ELEMENT: "IEDERE INFORMATIE" 6

2. TWEEDE ELEMENT: "BETREFFENDE" 9

3. DERDE ELEMENT: "GEÏDENTIFICEERDE OF IDENTIFICEERBARE" [NATUURLIJKE PERSOON] 13

4. VIERDE ELEMENT: "NATUURLIJKE PERSOON" 23

IV. WAT ALS GEGEVENS NIET ONDER DE DEFINITIE VALLEN? 25

V. CONCLUSIES 26

I. INLEIDING

De Groep is zich bewust van de noodzaak van een diepgaande analyse van het begrip "persoonsgegeven". Informatie over de huidige praktijk in de EU-lidstaten lijkt te wijzen op enige onzekerheid over en een van lidstaat tot lidstaat uiteenlopende toepassing van belangrijke aspecten van dit begrip, wat invloed kan hebben op het goede functioneren van de gegevensbescherming in diverse contexten. De uitkomst van deze analyse van dit kernelement van de toepassing en interpretatie van de regels voor gegevensbescherming zal voor een aantal belangrijke kwesties indringende gevolgen hebben, en is bijzonder relevant voor thema's als identiteitsbeheer in de context van e-overheid en e-gezondheidzorg en in verband met RFID.

Dit advies van de Groep moet leiden tot een gemeenschappelijke visie op het begrip persoonsgegeven, en de situaties waarin en de wijze waarop de nationale wetgeving inzake gegevensbescherming moet worden toegepast. Het uitwerken van een gemeenschappelijke definitie van persoonsgegevens houdt in dat moet worden bepaald wat wel en wat niet onder de regelgeving voor gegevensbescherming valt. Als uitvloeisel van dat werk moeten richtsnoeren worden gegeven voor de wijze waarop de nationale regelgeving voor gegevensbescherming moet worden toegepast op bepaalde soorten situaties die in heel Europa voorkomen. Hiermee wordt bijgedragen tot de uniforme toepassing van dergelijke regelgeving, wat een van de kerntaken van de Groep Artikel 29 is.

Om de analyse te ondersteunen en illustreren worden in dit document voorbeelden gegeven die ontleend zijn aan het werk van de nationale autoriteiten voor gegevensbescherming in de EU. De meeste voorbeelden zijn uitsluitend aangepast voor het gebruik in dit verband.

II. ALGEMENE OVERWEGINGEN EN BELEIDSVRAGEN

Het begrip persoonsgegeven wordt in de richtlijn breed opgevat.

De definitie van persoonsgegevens in Richtlijn 95/46/EG (hierna "de richtlijn gegevensbescherming" of "de richtlijn" genoemd) luidt als volgt:

Onder "persoonsgegevens" wordt verstaan '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 elementen die kenmerkend zijn voor zijn fysieke, fysiologische, mentale, economische, culturele of sociale identiteit.'

Deze definitie weerspiegelt de bedoeling van de Europese wetgever een brede definitie van persoonsgegevens te geven, waaraan tijdens het gehele wetgevingsproces is vastgehouden. In het oorspronkelijke voorstel van de Commissie werd gesteld: *"Zoals in Verdrag nr. 108 wordt dit begrip ruim gedefinieerd, zodat daaronder alle gegevens vallen die in verband kunnen worden gebracht met een bepaalde persoon."*[2]. In het gewijzigde voorstel van de Commissie wordt opgemerkt: *"Het gewijzigde voorstel komt tegemoet aan de wens van het Parlement om een zo algemeen mogelijke definitie van het begrip 'persoonsgegeven' te hanteren, die van toepassing is op alle informatie die op een natuurlijke persoon betrekking kan hebben"*[3]. Ook de Raad hield in zijn gemeenschappelijk standpunt[4] met die wens rekening.

Het doel van de regels in de richtlijn is de bescherming van personen.

In artikel 1 van Richtlijn 95/46/EG en Richtlijn 2002/58/EG wordt het uiteindelijke doel van de regels duidelijk verwoord: bij de verwerking van persoonsgegevens moet de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen worden gewaarborgd, met name het recht op een persoonlijke levenssfeer. Dit is een belangrijk punt waarmee rekening moet worden gehouden bij de interpretatie en toepassing van de regels die in beide instrumenten zijn vervat. Het kan een aanzienlijke rol spelen bij de vaststelling hoe de bepalingen van de richtlijn moeten worden toegepast op sommige situaties waarbij geen risico bestaat voor de rechten van personen; bovendien kan het ervoor hoeden dat de regels zo worden geïnterpreteerd dat personen de bescherming van hun rechten wordt ontnomen.

Sommige activiteiten zijn van het toepassingsgebied van de richtlijn uitgesloten, en de tekst voorziet in de nodige flexibiliteit om een passend juridisch antwoord te kunnen geven op de omstandigheden van een bepaald geval.

Hoewel de richtlijn een ruime definitie van "persoonsgegeven" en "verwerking" hanteert, betekent het loutere feit dat een situatie "verwerking van persoonsgegevens" in de zin van de richtlijn kan worden geacht in te houden, op zich nog niet dat die situatie onderworpen moet zijn aan de regels van de richtlijn, met name gezien het bepaalde in artikel 3. Naast het feit dat bepaalde situaties niet binnen de werkingssfeer van het Gemeenschapsrecht vallen, worden in artikel 3 ontheffingen geformuleerd die verband houden met de technische wijze van

---

2 COM(90) 314 def. van 13.9.1990, blz. 15 (toelichting op artikel 2).

3 COM(92) 422 def. van 28.10.1992, blz. 23 (toelichting op artikel 2).

4 Gemeenschappelijk Standpunt (EG) nr. 1/95 door de Raad vastgesteld op 20 februari 1995 (PB C 93 van 13.4.1995, blz. 20).

verwerking (indien die in handmatige niet-gestructureerde vorm gebeurt) en het doel waarvoor de gegevens worden verwerkt (indien een natuurlijke persoon de verwerking verricht in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden). Ook indien de verwerking van persoonsgegevens binnen de werkingssfeer van de richtlijn valt, kan het zijn dat niet alle daarin vervatte regels in een bepaald geval van toepassing zijn. Een aantal bepalingen van de richtlijn biedt een aanzienlijke mate van flexibiliteit, zodat een passende afweging kan worden gemaakt tussen enerzijds de bescherming van de rechten van de betrokkene en anderzijds de rechtmatige belangen van de voor de verwerking verantwoordelijke en van derden, en mogelijke algemene belangen. Dergelijke bepalingen zijn bijvoorbeeld te vinden in artikel 6 (de bewaringsduur is afhankelijk van de vraag hoe lang bewaring noodzakelijk is), artikel 7, onder f) (voor de rechtvaardiging van de verwerking wordt een afweging van de betrokken belangen gemaakt), artikel 10, onder c), laatste streepje, artikel 11, lid 1, onder c) (informatieverstrekking aan de betrokkene wanneer dat nodig is om eerlijke verwerking te waarborgen) en artikel 18 (vrijstellingen van de verplichting tot aanmelding).

De reikwijdte van de regels voor gegevensbescherming moet niet te ver worden opgerekt.

Het zou ongewenst zijn als de regels voor gegevensbescherming worden toegepast op situaties waarvan het niet de bedoeling was ze onder die regels te laten vallen, en waarvoor die regels door de wetgever ook niet zijn opgezet. De genoemde materiële uitzonderingen uit hoofde van artikel 3 en de verduidelijkingen in de overwegingen 26 en 27 van de richtlijn laten zien hoe de wetgever wenste dat de gegevensbescherming zou worden toegepast.

Een van de beperkingen houdt verband met de wijze waarop gegevens worden verwerkt. De reden waarom in de jaren zeventig de eerste wetgeving inzake gegevensbescherming werd uitgevaardigd, was immers dat met nieuwe technologieën, zoals elektronische gegevensverwerking, persoonsgegevens eenvoudiger en in ruimere mate toegankelijk konden worden gemaakt dan met de traditionele methoden voor gegevensverwerking. De gegevensbescherming waarin de richtlijn voorziet, is derhalve gericht op de bescherming van vormen van verwerking die gekenmerkt worden door een groter risico in verband met de gemakkelijke toegang tot persoonsgegevens (overweging 27). Niet-geautomatiseerde verwerking van persoonsgegevens valt alleen binnen de werkingssfeer van de richtlijn indien die gegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen (artikel 3).

Een andere algemene beperking van de toepasselijkheid van de richtlijn betreft de verwerking van gegevens in zodanige omstandigheden dat mag worden aangenomen dat middelen om de betrokkene te identificeren niet “redelijkerwijs […] in te zetten zijn” (overweging 26). Dit onderwerp zal later nader worden besproken.

Ook moet echter worden voorkomen dat de interpretatie van het begrip persoonsgegevens onterecht wordt ingeperkt.

Wanneer een mechanische toepassing van elke bepaling van de richtlijn op het eerste gezicht al te belastende of wellicht zelfs absurde consequenties zou hebben, moet eerst worden nagegaan of 1) de situatie wel binnen de werkingssfeer van de richtlijn valt, met name gezien artikel 3, en 2), als de situatie binnen de werkingssfeer van de richtlijn valt, of de richtlijn zelf of de nationale wetgeving die ingevolge de richtlijn is vastgesteld, voorziet in ontheffingen of vereenvoudigde procedures voor bepaalde situaties om tot een passend juridisch antwoord te komen zonder de bescherming van de rechten van de betrokkenen en de op het spel staande belangen onrecht te doen. Het is beter de interpretatie van de definitie van persoonsgegeven

niet onnodig te beperken, maar in het oog te houden dat er aanzienlijke ruimte is voor een flexibele toepassing van de regels op dergelijke gegevens.

De nationale toezichthoudende autoriteiten voor gegevensbescherming spelen in dit verband een essentiële rol in het kader van hun taak om toezicht te houden op de toepassing van de wetgeving inzake gegevensbescherming, die inhoudt dat zij wetsbepalingen interpreteren en concrete richtsnoeren geven voor de voor de verwerking verantwoordelijken en de betrokkenen. Zij moeten bevorderen dat een definitie tot stand komt die breed genoeg is om toekomstige ontwikkelingen en alle mogelijke grijze zones te kunnen ondervangen, terwijl legitiem gebruik wordt gemaakt van de flexibiliteit die de richtlijn biedt. De tekst van de richtlijn nodigt uit tot de formulering van een beleid dat een ruime interpretatie van het begrip persoonsgegeven combineert met een passend evenwicht bij de toepassing van de bepalingen van de richtlijn.

III. ANALYSE VAN DE DEFINITIE VAN PERSOONSGEGEVEN IN DE RICHTLIJN GEGEVENSBESCHERMING

De definitie in de richtlijn is opgebouwd uit vier elementen, die hier ieder afzonderlijk worden besproken. Die elementen zijn:

– “iedere informatie”

– “betreffende”

– “geïdentificeerd of identificeerbaar”

– “natuurlijke persoon”

Deze vier elementen zijn onderling nauw vervlochten en van elkaar afhankelijk. In verband met de in dit document gevolgde methode wordt elk van de elementen echter afzonderlijk behandeld.

1. EERSTE ELEMENT: “IEDERE INFORMATIE”

Uit het gebruik van de term “iedere informatie” blijkt duidelijk dat de wetgever een ruime definitie van het begrip “persoonsgegeven” heeft willen geven. Deze woordkeuze vraagt om een ruime interpretatie.

Wat de aard van de informatie betreft, omvat “persoonsgegeven” alle soorten uitspraken over een persoon. Er valt “objectieve” informatie onder, zoals de aanwezigheid van een bepaalde substantie in iemands bloed. Ook “subjectieve” informatie, meningen en oordelen vallen eronder. Het laatste type uitspraken maakt een aanzienlijk deel uit van de persoonsgegevens die verwerkt worden in sectoren als het bankwezen, aangaande de betrouwbaarheid van leningnemers (“Titius is een betrouwbare debiteur”), het verzekeringswezen (“Titius zal naar verwachting niet spoedig overlijden”) of bij de werkgever (“Titius werkt hard en verdient bevorderd te worden”).

Om als “persoonsgegeven” te worden aangemerkt, is het niet nodig dat de informatie waar is of bewezen. De regels voor gegevensbescherming houden rekening met de mogelijkheid dat

informatie onjuist is en geven de betrokkene het recht op toegang tot die informatie en voorzien in rechtsmiddelen om die te doen corrigeren[5].

Wat de inhoud van de informatie betreft, omvatten "persoonsgegevens" gegevens die welke soort informatie dan ook geven. Hiertoe behoort uiteraard persoonlijke informatie die als gevoelig wordt beschouwd (artikel 8 van de richtlijn) omdat zij door de aard ervan bijzondere risico's met zich meebrengt, maar ook meer algemene soorten informatie. "Persoonsgegevens" omvatten informatie die betrekking heeft op iemands privéleven of familie- en gezinsleven in strikte zin, maar ook informatie over allerlei activiteiten die iemand onderneemt, bijvoorbeeld over iemands beroepsrelaties of economisch of sociaal gedrag. Het gaat hier dus om informatie over personen, ongeacht de positie of de hoedanigheid van die personen (consument, patiënt, werknemer, klant, enz.).

Voorbeeld 1: gewoonten en werkwijzen bij de beroepsuitoefening

Informatie over het voorschrijven van geneesmiddelen (bijvoorbeeld identificatienummer van het geneesmiddel, naam van het geneesmiddel, gehalte van de werkzame stof, fabrikant, verkoopprijs, eerste recept of herhalingsrecept, redenen voor het gebruik, redenen waarom geen vervangend geneesmiddel geschikt is, naam, voornaam en telefoonnummer van de voorschrijvende arts, enz.), of het nu gaat om een bepaald afzonderlijk recept of om patronen in het voorschrijfgedrag van de arts, kan als een persoonsgegeven worden beschouwd betreffende de voorschrijvende arts, ook als de patiënt anoniem is. Wanneer informatie over door geïdentificeerde of identificeerbare artsen uitgeschreven recepten wordt verstrekt aan producenten van geneesmiddelen die alleen op recept verkrijgbaar zijn, is er derhalve sprake van verstrekking van persoonsgegevens aan derden als bedoeld in de richtlijn.

Deze interpretatie wordt ondersteund door de formulering van de richtlijn zelf. Enerzijds moet in aanmerking worden genomen dat het begrip privéleven en familie- en gezinsleven ruim moet worden opgevat, zoals het Europees Hof voor de rechten van de mens duidelijk heeft gemaakt[6]. Anderzijds houden de regels voor de bescherming van persoonsgegevens meer in dan de bescherming van het begrip in ruime zin van het recht op respect voor het privé- en gezins- en familieleven. In het Handvest van de grondrechten van de Europese Unie is de bescherming van persoonsgegevens gewaarborgd in artikel 8 als autonoom recht, naast en afzonderlijk van het recht op eerbiediging van het privéleven en het familie- en gezinsleven in artikel 7. Hetzelfde geldt in sommige lidstaten op nationaal niveau. Dit is in overeenstemming met artikel 1, lid 1, van de richtlijn, dat spreekt van "de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, *inzonderheid* [maar niet uitsluitend] van het recht op persoonlijke levenssfeer". De richtlijn verwijst dan ook afzonderlijk naar de verwerking van persoonsgegevens in contexten buiten de sfeer van de woning en het familie- en gezinsleven, zoals in het kader van het arbeidsrecht (artikel 8, lid 2, onder b)), bij strafrechtelijke veroordelingen, administratieve sancties en burgerrechtelijke beslissingen

5 Rectificatie is mogelijk door het toevoegen van andersluidende opmerkingen of door passende rechtsmiddelen, zoals beroepsprocedures.

6 Arrest van het Europees Hof voor de rechten van de mens in de zaak Amann/Zwitserland van 16.2.2000, § 65: *"[…] de term "privéleven" mag niet restrictief worden uitgelegd. In het bijzonder omvat respect voor het privéleven het recht betrekkingen met andere mensen tot stand te brengen en te ontwikkelen; bovendien is er geen principiële reden om activiteiten van professionele of zakelijke aard van het begrip "privéleven" uit te sluiten (zie het arrest in de zaak Niemietz/Duitsland van 16 december 1992, Serie A nr. 251-B, blz. 33–34, § 9 en het eerder geciteerde arrest in de zaak Halford, blz. 1015–16, § 42). Die ruime interpretatie stemt overeen met die van het Verdrag van de Raad van Europa van 28 januari 1981 […]".*

(artikel 8, lid 5) of direct marketing (artikel 14, onder b)). Het Hof van Justitie van de Europese Gemeenschappen[7] heeft deze brede aanpak goedgekeurd.

Wat betreft de vorm waarin of het medium waarop de informatie is opgenomen, omvat het begrip persoonsgegeven informatie in welke vorm dan ook, bijvoorbeeld alfanumeriek, grafisch, fotografisch of akoestisch. Hiertoe behoort ook informatie op papier, alsmede informatie die bijvoorbeeld in binaire code in een computergeheugen is opgeslagen of op videoband. Dit is een logisch gevolg van het feit dat de automatische verwerking van persoonsgegevens binnen de werkingssfeer van de richtlijn valt. Met name geluids- en beeldgegevens gelden vanuit dit standpunt als persoonsgegevens, voor zover zij informatie over een persoon geven. Dat in artikel 33 van de richtlijn in het bijzonder naar geluids- en beeldgegevens wordt verwezen, moet in dit verband worden gezien als bevestiging en verduidelijking van het feit dat dergelijke gegevens inderdaad binnen de werkingssfeer van de richtlijn vallen (mits aan alle andere voorwaarden is voldaan) en dat de richtlijn erop van toepassing is. Dat is een logische veronderstelling voor het bepaalde in dat artikel, dat bedoeld is om tot een oordeel te komen over de vraag of de regels van de richtlijn voor die bepaalde gebieden een passende juridische respons bieden. Dit wordt nader verduidelijkt in overweging 14, waarin wordt gesteld dat *"gezien het belang van de in het kader van de informatiemaatschappij aan de gang zijnde ontwikkelingen inzake de technieken voor het opvangen, doorsturen, manipuleren, registreren, bewaren of mededelen van geluid- en beeldgegevens betreffende natuurlijke personen, deze richtlijn ook van toepassing zal moeten zijn op verwerkingen die op deze gegevens betrekking hebben"*. Om te worden beschouwd als een persoonsgegeven, is het anderzijds niet noodzakelijk dat informatie is opgenomen in een gestructureerde database of een gegevensbestand. Ook informatie die in vrije tekst in een elektronisch document voorkomt, kan als een persoonsgegeven worden aangemerkt, indien aan de andere criteria van de definitie van persoonsgegeven is voldaan. E-mail zal bijvoorbeeld "persoonsgegevens" bevatten.

Voorbeeld 2: telefonisch bankieren

Wanneer bij telefonisch bankieren de klant gesproken instructies geeft aan de bank en deze instructies op band worden opgenomen, moeten de opgenomen instructies als persoonsgegevens worden beschouwd.

Voorbeeld 3: videobewaking

Beelden van personen die door een videobewakingssysteem zijn geregistreerd, kunnen persoonsgegevens zijn, voor zover de personen herkenbaar zijn.

Voorbeeld 4: een kindertekening

In het kader van een gerechtelijke procedure betreffende de voogdij over een kind wordt een neuropsychiatrisch onderzoek van het betrokken meisje uitgevoerd, waarbij een door haar gemaakte tekening van haar gezin wordt voorgelegd. De tekening geeft informatie over de gemoedstoestand van het kind en over haar gevoelens betreffende de verschillende leden van het gezin. De tekening kan daarom als "persoonsgegeven" worden beschouwd. De tekening

[7] Arrest van het Hof van Justitie in de zaak C-101/2001 van 6.11.2003 (Lindqvist), punt 24: *"Het in artikel 3, lid 1, van Richtlijn 95/46 gebezigde begrip persoonsgegevens omvat volgens de definitie in artikel 2, sub a, daarvan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen."*

geeft namelijk informatie over het kind (haar gezondheidstoestand vanuit psychiatrisch gezichtspunt) en ook over het gedrag van bijvoorbeeld haar vader of moeder. De ouders kunnen in dit geval dan ook hun recht op toegang tot dit specifieke stuk informatie doen gelden.

In dit verband moet speciale melding worden gemaakt van biometrische gegevens. Dergelijke gegevens kunnen worden gedefinieerd als biologische eigenschappen, fysiologische kenmerken, gedragseigenschappen of herhaalbare handelingen, waarbij die kenmerken en/of handelingen zowel uniek voor de betreffende persoon als meetbaar zijn, ook indien er bij de patronen die in de praktijk worden toegepast om ze technisch te meten, sprake is van een zekere mate van waarschijnlijkheid. Typische voorbeelden van biometrische gegevens zijn vingerafdrukken, netvliesscans, gelaatskenmerken, stemkenmerken, maar ook de geometrie van de hand, bloedvatpatronen of zelfs vaste gewoonten of andere gedragskenmerken (zoals een geschreven handtekening, toetsaanslagpatronen, een bepaalde wijze van lopen of spreken, enz.).

Een kenmerk van biometrische gegevens is dat ze als de *inhoud* van de informatie over een bepaalde persoon kunnen worden beschouwd (Titius heeft bepaalde vingerafdrukken), maar ook als een element dat een koppeling tot stand brengt tussen een gegeven en een persoon (dit voorwerp is aangeraakt door een persoon met bepaalde vingerafdrukken, en die vingerafdrukken stemmen overeen met die van Titius; dus is dit voorwerp aangeraakt door Titius). Ze kunnen daardoor als identificatiemiddelen fungeren. Doordat ze op unieke wijze zijn gekoppeld aan een specifieke persoon, kunnen biometrische gegevens dan ook worden gebruikt om die persoon te identificeren. Deze tweeledige aard geldt ook voor DNA-gegevens, die informatie verstrekken over het menselijk lichaam en ook de ondubbelzinnige en unieke identificatie van een persoon mogelijk maken.

Monsters van menselijk weefsel (bijvoorbeeld een bloedmonster) fungeren als de bron waaruit de biometrische gegevens worden afgeleid, maar zijn zelf geen biometrisch gegeven (zoals bijvoorbeeld een vingerafdruk een biometrisch gegeven is, maar de vinger zelf niet). Het afleiden van informatie uit een monster valt derhalve onder het verzamelen van persoonsgegevens, waarop de richtlijn van toepassing is. Voor het verzamelen, de opslag en het gebruik van weefselmonsters zelf kunnen afzonderlijke regels gelden[8].

2. TWEEDE ELEMENT: "BETREFFENDE"

Dit is een cruciaal element van de definitie, omdat het uiterst belangrijk is exact na te gaan welke verhoudingen/verbanden van belang zijn en hoe die moeten worden onderscheiden.

In algemene termen kan informatie worden geacht een persoon te "betreffen" wanneer het om informatie *over* die persoon gaat.

In vele gevallen kan dit "betreffen" gemakkelijk worden vastgesteld. De gegevens die zijn opgenomen in iemands persoonlijk dossier bij de afdeling personeelszaken "betreffen" bijvoorbeeld duidelijk de situatie van die persoon als werknemer. Hetzelfde geldt voor de resultaten van een medisch onderzoek van een patiënt die in diens patiëntendossier zijn opgenomen, of de afbeelding van een persoon die in een video-interview met die persoon is opgenomen.

---

[8] Zie Aanbeveling nr. Rec. (2006) 4 aan de lidstaten van het Comité van Ministers van de Raad van Europa van 15 maart 2006 over het onderzoek aan biologische materialen van menselijke oorsprong.

Er zijn echter ook situaties waarin het niet altijd zo duidelijk is als in de voornoemde gevallen om te bepalen dat de informatie iemand "betreft".

Soms gaat het bij de informatie die in de gegevens is vervat in eerste instantie om voorwerpen en niet om personen. Die voorwerpen zijn doorgaans iemands eigendom, staan onder het beheer van of oefenen invloed uit op een persoon, of staan in een bepaalde fysieke of geografische nabijheidsrelatie tot personen of andere voorwerpen. De informatie kan in dergelijke gevallen slechts indirect geacht worden die personen of voorwerpen te betreffen.

Voorbeeld 5: de waarde van een woning

Bij de waarde van een bepaalde woning gaat het om informatie over een voorwerp. De regels inzake gegevensbescherming zijn duidelijk niet van toepassing wanneer die informatie uitsluitend wordt gebruikt ter illustratie van de hoogte van de huizenprijzen in een bepaald gebied. In bepaalde omstandigheden kan deze informatie echter wel als persoonsgegeven worden beschouwd. Het huis behoort tot het vermogen van de eigenaar, en dit gegeven wordt dan ook gebruikt om bijvoorbeeld de omvang van de belastingverplichtingen van de eigenaar te bepalen. In een dergelijke context moet deze informatie ongetwijfeld als persoonsgegeven worden beschouwd.

Een soortgelijke analyse kan worden gemaakt wanneer de gegevens betrekking hebben op processen of gebeurtenissen, bijvoorbeeld informatie over het functioneren van een machine waarvoor menselijk ingrijpen is vereist. In bepaalde omstandigheden kan dergelijke informatie ook worden geacht een persoon te "betreffen".

Voorbeeld 6: onderhoudsregister van auto's

Het onderhoudsregister dat een automonteur of garagehouder bijhoudt, bevat informatie over de onderhouden auto, de kilometerstand, de data van de onderhoudsbeurten, technische problemen en de toestand van het voertuig. Deze informatie is in het register gekoppeld aan het kenteken en het chassisnummer, die weer kunnen worden teruggevoerd op de eigenaar. Wanneer de garage een koppeling aanbrengt tussen het voertuig en de eigenaar met het oog op de facturering, is er sprake van informatie "betreffende" de eigenaar of de bestuurder. Indien een koppeling wordt aangebracht met de monteur die aan de auto heeft gewerkt, om diens arbeidsproductiviteit te kunnen vaststellen, is er ook weer sprake van informatie "betreffende" de monteur.

De Groep heeft al eerder aandacht besteed aan de vraag wanneer informatie kan worden beschouwd als informatie "betreffende" een persoon. In de context van de discussie over de problemen op het gebied van gegevensbescherming die samenhangen met RFID-tags merkte de Groep op dat *gegevens iemand betreffen wanneer zij verwijzen naar de identiteit, de kenmerken of het gedrag van een persoon of indien dergelijke informatie wordt gebruikt om de wijze waarop die persoon wordt behandeld of beoordeeld te bepalen of te beïnvloeden*[9].

Gezien de hierboven vermelde gevallen en volgens dezelfde gedachtegang kan worden gesteld dat om te kunnen spreken van gegevens "betreffende" iemand, er sprake moet zijn van een van de drie volgende elementen: "**inhoud**" OF "**doel**" OF "**resultaat**".

---

9 Document WP 105 van de Groep Artikel 29: "Werkdocument inzake problemen op het gebied van gegevensbescherming die verband houden met de RFID-technologie", goedgekeurd op 19 januari 2005, blz. 8.

Het element "**inhoud**" is aanwezig wanneer – volgens de meest voor de hand liggende en gebruikelijke opvatting in een samenleving van het woord "betreffende" – informatie wordt gegeven over een bepaalde persoon, ongeacht het doel dat de voor de verwerking verantwoordelijke of een derde daarmee beoogt en ongeacht de gevolgen van die informatie voor de betrokkene. Er is sprake van informatie "betreffende" een persoon wanneer het gaat om informatie "over" die persoon, wat beoordeeld moet worden in het licht van alle omstandigheden van het geval. De resultaten van een medisch onderzoek betreffen duidelijk de patiënt, net zoals de informatie die een bedrijf aanhoudt in het dossier dat de naam van een bepaalde klant draagt, duidelijk die klant betreft. Ook de informatie die vervat is in een RFID-tag of een streepjescode, opgenomen in iemands identiteitsdocument, betreft die persoon (zoals in de komende paspoorten die een RFID-chip bevatten).

Ook het element "**doel**" kan ervoor zorgen dat informatie een bepaalde persoon "betreft". Dit "doel" kan worden geacht te bestaan wanneer, rekening houdende met alle omstandigheden van het precieze geval, gegevens worden gebruikt of waarschijnlijk zullen worden gebruikt met het doel een persoon te beoordelen, op een bepaalde wijze te behandelen of de status of het gedrag van die persoon te beïnvloeden.

Voorbeeld 7: gespreksregister van een telefoon

Het gespreksregister van een telefoon in een kantoorgebouw geeft informatie over de gesprekken die zijn gevoerd met die telefoon en de lijn waarmee het toestel is verbonden. Die informatie kan met verschillende punten in verband worden gebracht. Enerzijds is het zo dat de lijn beschikbaar is gesteld aan het bedrijf, dat contractueel verplicht is voor de gevoerde gesprekken te betalen. De telefoon is gedurende werktijd in beheer bij een bepaalde werknemer, en de gesprekken worden geacht door hem te zijn gevoerd. Het gespreksregister kan ook informatie geven over de persoon die is gebeld. Het telefoontoestel kan ook worden gebruikt door iedereen die toegang heeft tot het vertrek wanneer de werknemer afwezig is (bijvoorbeeld schoonmakers). De informatie over het gebruik van het toestel kan dus, met verschillende doeleinden, in verband worden gebracht met het bedrijf, de werknemer, het schoonmaakpersoneel (bijvoorbeeld om te controleren hoe laat de schoonmakers van hun werk vertrekken, aangezien zij geacht worden telefonisch te melden wanneer zij vertrekken, voor het gebouw wordt afgesloten). Het begrip persoonsgegeven strekt zich in dit verband uit tot zowel binnenkomende als uitgaande gesprekken, aangezien beide informatie bevatten over het privéleven van personen en hun maatschappelijke betrekkingen en contacten.

Een derde type "betreffen" ten aanzien van specifieke personen ontstaat door de aanwezigheid van het element "**resultaat**". Ook als de elementen "inhoud" of "doel" ontbreken, kunnen gegevens geacht worden iemand te "betreffen" indien het gebruik ervan, rekening houdende met alle omstandigheden van het geval, naar verwachting gevolgen zal hebben voor iemands rechten of belangen. Het is daarbij niet noodzakelijk dat het bij het potentiële resultaat gaat om grote gevolgen. Het is voldoende als de persoon als gevolg van de verwerking van de betrokken gegevens anders wordt behandeld dan anderen.

Voorbeeld 8: volgen van de positie van taxi's ter verbetering van de dienstverlening, met gevolgen voor de chauffeurs

Een taxibedrijf gebruikt een systeem voor positiebepaling per satelliet, waarmee de positie van de beschikbare taxi's in werkelijke tijd kan worden vastgesteld. Het doel van de verwerking is betere dienstverlening en brandstofbesparing, doordat wanneer een klant een taxi bestelt, de dichtstbijzijnde wagen naar zijn adres wordt gestuurd. Strikt genomen gaat het bij dit systeem om gegevens betreffende de taxi's en niet betreffende de taxichauffeurs. Het doel van de verwerking is niet de beoordeling van de prestaties van de taxichauffeurs, bijvoorbeeld door optimalisering van hun routes. Het systeem maakt het echter mogelijk toezicht te houden op de prestaties van de taxichauffeurs en na te gaan of zij zich aan snelheidsbeperkingen houden, de juiste routes kiezen, zich achter het stuurwiel bevinden of buiten de taxi aan het rusten zijn, enz. Omdat er dus aanzienlijke gevolgen kunnen zijn voor deze personen, kunnen de gegevens ook worden beschouwd als gegevens betreffende natuurlijke personen. Voor de verwerking moeten dus de regels inzake gegevensbescherming gelden.

Deze drie elementen (inhoud, doel, resultaat) moeten worden beschouwd als alternatieve voorwaarden, niet als cumulatieve voorwaarden. Met name is het zo, dat wanneer het element "inhoud" aanwezig is, er sprake is van informatie betreffende een persoon, ook als de andere elementen niet aanwezig zijn. Een gevolg hiervan is dat dezelfde informatie tegelijkertijd verschillende personen kan betreffen, afhankelijk van welk element met betrekking tot elk van hen aanwezig is. Dezelfde informatie kan, vanwege het element "inhoud", de persoon Titius betreffen (het zijn duidelijk gegevens over Titius) EN, vanwege het element "doel", de persoon Gaius (de gegevens worden gebruikt teneinde Gaius op een of andere manier te behandelen) EN, vanwege het element "resultaat", de persoon Sempronius (de informatie zal waarschijnlijk gevolgen hebben voor de rechten en belangen van Sempronius). Om te kunnen spreken van informatie betreffende een bepaalde persoon is het dus niet noodzakelijk dat de informatie op die persoon "gericht" is. Uit het voorgaande volgt dat de vraag of gegevens een bepaalde persoon betreffen voor elk afzonderlijk gegeven op zijn eigen merites moet worden beoordeeld. Bij de toepassing van inhoudelijke bepalingen (bijvoorbeeld waar het gaat om wie recht heeft op toegang tot de gegevens) moet eveneens rekening worden gehouden met het feit dat informatie verschillende personen kan betreffen.

Voorbeeld 9: informatie die in de notulen van een vergadering is opgenomen

Een voorbeeld waaruit blijkt dat, zoals hierboven uiteengezet, elk gegeven afzonderlijk moet worden beoordeeld, betreft de informatie die is opgenomen in de notulen van een vergadering, waarin zijn opgenomen: de aanwezigheid van de deelnemers Titius, Gaius en Sempronius, uitspraken die zijn gedaan door Titius en Gaius en een verslag van de besprekingen over bepaalde onderwerpen, zoals samengevat door de notulist Sempronius. Als persoonsgegeven betreffende Titius kan alleen worden beschouwd de informatie dat hij de vergadering op een bepaalde tijd en plaats heeft bijgewoond, en dat hij daar bepaalde uitspraken heeft gedaan. De aanwezigheid op de vergadering van Gaius, diens uitspraken en de samenvatting door Sempronius van de besprekingen over een bepaald onderwerp zijn GEEN persoonsgegevens betreffende Titius. Dit is ook het geval indien deze informatie in hetzelfde document is opgenomen, en zelfs als het onderwerp door Titius voor bespreking tijdens de vergadering is voorgedragen. Derhalve zijn deze punten uitgesloten van Titius' recht op toegang tot zijn eigen persoonsgegevens. Of en in hoeverre de informatie kan worden beschouwd als persoonsgegevens betreffende Gaius en Sempronius moet afzonderlijk worden beoordeeld op de hierboven omschreven wijze.

3. DERDE ELEMENT: "GEÏDENTIFICEERDE OF IDENTIFICEERBARE" [NATUURLIJKE PERSOON]

Overeenkomstig de richtlijn moet het gaan om informatie betreffende een "geïdentificeerde of identificeerbare" natuurlijke persoon. Dit geeft aanleiding tot de hiernavolgende overwegingen.

In algemene termen kan een natuurlijke persoon als "geïdentificeerd" worden beschouwd als hij of zij binnen een groep personen wordt "onderscheiden" van alle andere leden van de groep. Analoog is een natuurlijke persoon "identificeerbaar" als die persoon weliswaar nog niet is geïdentificeerd, maar wel geïdentificeerd kan worden (dit is de betekenis van het achtervoegsel "-baar"). Dit tweede geval is dus in de praktijk de minimale voorwaarde die bepaalt of informatie onder het derde element valt.

Identificatie geschiedt normaliter door middel van bepaalde informatie-eenheden die we "identificatiemiddelen" kunnen noemen, en die tot de betrokken persoon in een bijzondere en nauwe relatie staan. Voorbeelden daarvan zijn de uiterlijke kenmerken van deze persoon, zoals lengte, haarkleur, kleding en dergelijke, of een eigenschap van de betrokkene die niet onmiddellijk kan worden waargenomen, zoals beroep, functie, naam en dergelijke. De richtlijn noemt deze identificatiemiddelen in de definitie van persoonsgegevens in artikel 2, waar wordt bepaald dat *"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 elementen die kenmerkend zijn voor zijn fysieke, fysiologische, mentale, economische, culturele of sociale identiteit"*.

"Direct" of "indirect" identificeerbaar

Een nadere verklaring is opgenomen in de toelichting bij de artikelen van het gewijzigde Commissievoorstel: *"Een persoon kan ofwel direct geïdentificeerd worden aan de hand van een naam ofwel indirect aan de hand van een telefoonnummer, een autokenteken, een sofi- of soortgelijk nummer, een paspoort dan wel met behulp van een aantal significante criteria, aan de hand waarvan zijn of haar identiteit binnen bijvoorbeeld een kleine groep kan worden vastgesteld (leeftijd, functie, adres, enz.)."*. Uit deze toelichting blijkt duidelijk dat de mate waarin een identificatiemiddel voldoende is om identificatie tot stand te brengen, afhankelijk is van de context van het geval. Een veel voorkomende familienaam is niet voldoende om iemand te identificeren – dat wil zeggen hem te onderscheiden – onder de gehele bevolking van een land, terwijl die naam wel voldoende is voor de identificatie van een bepaalde leerling in een schoolklas. Zelfs bijkomstige informatie, zoals "die man met een zwart pak aan", kan iemand identificeren temidden van voorbijgangers die bij een stoplicht staan te wachten. De vraag of de persoon wie de informatie betreft, daardoor al dan niet is geïdentificeerd, hangt dus af van de omstandigheden van het geval.

Waar het gaat om direct geïdentificeerde of identificeerbare personen is de **naam** inderdaad het meest gebruikelijke identificatiemiddel; in de praktijk wordt met "geïdentificeerde persoon" meestal gedoeld op diens naam.

Om iemands identiteit vast te stellen, moet de naam soms gecombineerd worden met andere informatie (geboortedatum, naam van de ouders, adres, foto van het gezicht) om verwarring met mogelijke naamgenoten te voorkomen. De informatie dat Titius een bepaalde som geld verschuldigd is, kan bijvoorbeeld worden geacht een geïdentificeerde persoon te betreffen, omdat die informatie is gekoppeld aan de naam van de betrokken persoon. De naam is een gegeven waaruit blijkt dat de drager ervan die combinatie van letters en klanken gebruikt om

zichzelf te onderscheiden en door anderen te worden onderscheiden van andere personen met wie hij betrekkingen onderhoudt. De naam kan ook het beginpunt zijn dat tot informatie leidt over waar iemand woont of verblijft en kan informatie geven over de personen die tot zijn familie behoren (door middel van de familienaam) en een aantal juridische en sociale verbanden die met die naam geassocieerd zijn (genoten onderwijs, medisch dossier, bankrekeningen). Het kan zelfs mogelijk zijn iemands uiterlijk te achterhalen, indien met de naam een afbeelding is geassocieerd. Al deze nieuwe, aan de naam gekoppelde gegevens kunnen het mogelijk maken door te dringen tot een mens van vlees en bloed; door de identificatiemiddelen wordt de oorspronkelijke informatie geassocieerd met een natuurlijke persoon die van andere personen kan worden onderscheiden.

Bij "indirect" geïdentificeerde of identificeerbare personen gaat het doorgaans om een klein of groot aantal "unieke combinaties". In gevallen waarin het op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen één bepaalde persoon te onderscheiden, kan die persoon wellicht toch "identificeerbaar" zijn doordat aan de hand van die informatie in combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) de betrokkene van andere personen kan worden onderscheiden. De richtlijn spreekt in dit verband van "een of meer elementen die kenmerkend zijn voor zijn fysieke, fysiologische, mentale, economische, culturele of sociale identiteit". Sommige kenmerken zijn in zodanige mate uniek dat iemand zonder enige moeite kan worden geïdentificeerd ("de huidige premier van Spanje"), maar ook een combinatie van categoriale gegevens (leeftijdscategorie, regionale afkomst, enz.) kan in sommige omstandigheden ruim voldoende zijn, met name indien aanvullende informatie beschikbaar is. Dit verschijnsel is door statistici uitvoerig bestudeerd, aangezien zij altijd moeten vermijden dat de vertrouwelijkheid wordt geschonden.

Voorbeeld 10: fragmentarische informatie in de pers

Er wordt informatie gepubliceerd over een misdrijf dat in het verleden veel opzien heeft gebaard. In deze publicatie wordt geen van de traditionele identificatiemiddelen genoemd, met name geen naam of geboortedatum.

Het is echter niet onredelijk moeilijk extra informatie te vinden om te weten te komen wie de belangrijkste betrokkenen waren, bijvoorbeeld door kranten uit de desbetreffende periode erop na te slaan. Verondersteld kan worden dat het zeker niet ondenkbaar is dat iemand die moeite neemt (het doorzoeken van oude kranten) waardoor hij hoogstwaarschijnlijk achter de naam en andere kenmerken van de betrokkenen kan komen. De in de eerste alinea bedoelde informatie in dit voorbeeld kan dus zeker worden beschouwd als "informatie over een identificeerbare persoon" en is dus een persoonsgegeven.

Hier moet worden 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. De persoonlijkheid van de betrokkene kan op deze wijze worden achterhaald, zodat bepaalde besluiten aan hem of haar kunnen worden toegeschreven. Zonder zelfs maar naar de naam en het adres van de persoon te vragen, kan de betrokkene worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde

beslissingen aan hem of haar worden toegeschreven, omdat het voor het contactpunt voor de persoon (de computer) niet langer nodig is zijn of haar identiteit in enge zin bekend te maken. 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[10].

Het Europees Hof van Justitie heeft zich in een arrest uitgesproken in die zin "*dat het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als 'verwerking van persoonsgegevens' in de zin van […] Richtlijn 95/46/EG is aan te merken*"[11].

Voorbeeld 11: asielzoekers

Aan asielzoekers in een opvangcentrum die hun werkelijke naam geheim houden, is voor administratieve doeleinden een codenummer toegekend. Aan de hand van dit nummer kunnen zij worden geïdentificeerd en gegevens betreffende het verblijf van de asielzoeker in het centrum worden aan het nummer gekoppeld. Door een foto of andere biometrische indicatoren is er een nauw, onmiddellijk verband met de fysieke persoon, waardoor deze kan worden onderscheiden van andere asielzoekers en verschillende gegevens met hem kunnen worden verbonden. Die gegevens betreffen in dit geval een "geïdentificeerde" natuurlijke persoon.

In artikel 8, lid 7, van de richtlijn wordt bepaald: "De lidstaten stellen de voorwaarden vast waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt.". Opgemerkt moet worden dat in deze bepaling niets wordt gezegd over wat voor voorwaarden de lidstaten moeten vaststellen, hoewel de bepaling deel uitmaakt van het artikel over gevoelige gegevens. In overweging 33 worden dergelijke gegevens als volgt aangeduid: "*gegevens die wegens hun aard op de fundamentele vrijheden of op de persoonlijke levenssfeer inbreuk kunnen maken*". Redelijkerwijs kan worden vermoed dat de wetgever met betrekking tot nationale identificatienummers dezelfde bezorgdheid heeft gevoeld, aangezien deze zeer gemakkelijk en ondubbelzinnig verschillende gegevens over een bepaalde persoon met elkaar in verband kunnen brengen.

Wijze van identificatie

In overweging 26 van de richtlijn wordt bijzondere aandacht geschonken aan de term "identificeerbaar": "*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*". Dit houdt in dat een slechts hypothetische mogelijkheid om iemand te onderscheiden niet voldoende is om die persoon als "identificeerbaar" te beschouwen. Indien, rekening houdende met "*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*", die mogelijkheid niet bestaat of verwaarloosbaar is, mag de persoon niet als "identificeerbaar" worden beschouwd en geldt de informatie niet als "persoonsgegeven". Bij de toepassing van het criterium "*alle middelen*

[10] Verslag over de toepassing van de beginselen van gegevensbescherming in het kader van de wereldwijde communicatienetwerken, door Yves Poullet c.s., aan het comité T-PD van de Raad van Europa, punt 2.3.1., T-PD (2004) 04 final.

[11] Arrest van het Hof van Justitie in de zaak C-101/2001 van 6.11.2003 (Lindqvist), punt 27.

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" moet in het bijzonder rekening worden gehouden met alle relevante factoren. De kosten van identificatie zijn een van die factoren, maar niet de enige. Het beoogde doel, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico van organisatorische tekortkomingen (bijvoorbeeld inbreuken op de vertrouwelijkheidsplicht) en technische storingen moeten allemaal in aanmerking worden genomen. Het gaat hier echter niet om een statische test; er moet rekening worden gehouden met de stand van de technologie ten tijde van de verwerking en de mogelijkheden voor ontwikkeling gedurende de periode waarvoor de gegevens worden verwerkt. Wellicht is identificatie niet mogelijk met de middelen die momenteel redelijkerwijs in te zetten zijn. Als het de bedoeling is de gegevens slechts één maand te bewaren, kan dan niet worden verwacht dat identificatie tijdens de levensduur van de informatie mogelijk zal zijn, en hoeft de informatie niet als persoonsgegevens te worden beschouwd. Wil men de informatie echter tien jaar bewaren, dan moet de voor de verwerking verantwoordelijke rekening houden met de mogelijkheid dat wellicht identificatie na negen jaar wel mogelijk is, waardoor de informatie vanaf dat moment als persoonsgegeven geldt. Het systeem moet zich kunnen aanpassen wanneer dergelijke ontwikkelingen zich voordoen en zorgen dat tijdig passende technische en organisatorische maatregelen worden genomen.

Voorbeeld 12: publicatie van röntgenfoto's met de voornaam van de patiënt

Een röntgenfoto van een vrouw werd gepubliceerd in een wetenschappelijk tijdschrift met vermelding van de (zeer ongewone) voornaam van de vrouw. Door de combinatie van de voornaam van de vrouw en het feit dat haar familieleden en kennissen wisten dat zij aan een bepaalde ziekte leed, was de vrouw voor bepaalde mensen identificeerbaar; de röntgenfoto moet in dit geval daarom als persoonsgegeven worden beschouwd.

Voorbeeld 13: farmaceutische onderzoeksgegevens

Ziekenhuizen en artsen sturen uit patiëntendossiers afkomstige gegevens door aan een bedrijf met het oog op medisch onderzoek. De namen van de patiënten worden niet vermeld, maar alleen volgnummers die op willekeurige wijze aan elk klinisch geval zijn toegewezen met het oog op consistentie en om te voorkomen dat de gegevens van verschillende patiënten worden verwisseld. De namen van de patiënten zijn uitsluitend bekend bij de betrokken artsen, die door het medisch geheim zijn gebonden. De gegevens bevatten geen aanvullende informatie die door middel van combinatie identificatie van de patiënten mogelijk maakt. Bovendien zijn alle andere juridische, technische of organisatorische maatregelen genomen om te voorkomen dat de betrokkenen geïdentificeerd of identificeerbaar worden. In deze omstandigheden kan een gegevensbeschermingsautoriteit oordelen dat er bij de gegevensverwerking door het farmaceutisch bedrijf geen redelijkerwijs in te zetten middelen zijn waarmee de betrokkenen kunnen worden geïdentificeerd.

Een van de relevante factoren om te bepalen of er *redelijkerwijs in te zetten middelen* zijn om de betrokkenen te identificeren, is zoals eerder gezegd het doel dat de voor de verwerking verantwoordelijke met de verwerking beoogt. Nationale gegevensbeschermingsautoriteiten hebben te maken gehad met gevallen waarin enerzijds door de voor de verwerking verantwoordelijke werd aangevoerd dat slechts verspreide stukjes informatie werden verwerkt, zonder verwijzing naar een naam of een ander direct identificatiemiddel, en dat de gegevens niet als persoonsgegevens moesten worden beschouwd en daarom niet onder de regels voor gegevensbescherming vielen. Anderzijds heeft de verwerking van die informatie slechts nut als die het mogelijk maakt specifieke personen te identificeren en op een bepaalde

wijze te behandelen. 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.

Voorbeeld 14: videobewaking

Dit is met name relevant voor videobewaking. In die context wordt door de voor de verwerking verantwoordelijken vaak aangevoerd dat identificatie slechts zal plaatsvinden voor een gering percentage van het verzamelde materiaal en dat er dus vóór de identificatie in die paar gevallen plaatsvindt, geen sprake is van verwerking van persoonsgegevens. Het doel van videobewaking is echter de identificatie van de personen die op de videobeelden te zien zijn, in alle gevallen dat de voor de verwerking verantwoordelijke dat nodig acht. Het hele proces moet dan ook worden beschouwd als de verwerking van gegevens over identificeerbare personen, ook als sommige personen in de praktijk niet identificeerbaar zijn.

Voorbeeld 15: dynamische IP-adressen

De Groep Artikel 29 heeft aangegeven dat zij IP-adressen ziet als gegevens betreffende een identificeerbare persoon. Zij heeft daarover het volgende gezegd: "*internetaanbieders en beheerders van lokale netwerken [kunnen] zonder veel moeite internetgebruikers identificeren aan wie ze IP-adressen hebben verstrekt, doordat ze als regel systematisch de datum, het tijdstip, de duur en het verstrekte dynamische IP-adres van gebruikers in een logbestand vastleggen. Hetzelfde geldt voor internetdienstverleners die een logboek op de HTTP-server bijhouden. In deze gevallen is het buiten kijf dat men kan spreken van persoonsgegevens in de zin van artikel 2, onder a), van de richtlijn*"[12].

Vooral in die gevallen dat het IP-adres wordt verwerkt met het doel de gebruikers van de computer te identificeren (bijvoorbeeld door de houder van een auteursrecht die computergebruikers wil aanklagen wegens schending van intellectuele-eigendomsrechten), gaat de voor de verwerking verantwoordelijke ervan uit dat de "redelijkerwijs in te zetten middelen" voor de identificatie van de betrokkenen beschikbaar zullen zijn, bijvoorbeeld via de rechtbanken waarop een beroep wordt gedaan, anders zou het verzamelen van de informatie geen zin hebben. Deze informatie moet dan ook als persoonsgegeven worden beschouwd.

[12] WP 37: "Privacy op internet – Een geïntegreerde EU-aanpak van onlinegegevensbescherming", goedgekeurd op 21.11.2000.

In sommige gevallen is het voor bepaalde IP-adressen om diverse technische en organisatorische redenen niet mogelijk de gebruiker te identificeren. Een voorbeeld zijn de IP-adressen die zijn toegewezen aan computers in een internetcafé waar van de klanten geen legitimatie wordt verlangd. Hier zou kunnen worden aangevoerd dat de gegevens over het gebruik van computer X gedurende een bepaalde periode geen identificatie van de gebruiker met redelijkerwijs in te zetten middelen mogelijk maken en dat die gegevens daarom geen persoonsgegevens zijn. De internetdienstverlener zal echter naar alle waarschijnlijkheid niet weten of het IP-adres in kwestie identificatie mogelijk maakt, en zal de aan dat IP-adres gekoppelde gegevens op dezelfde wijze behandelen als informatie die gekoppeld is aan IP-adressen van geregistreerde en identificeerbare gebruikers. Tenzij de internetdienstverlener dus met absolute zekerheid gegevens van niet-identificeerbare gebruikers kan onderscheiden, zal hij alle IP-informatie voor alle zekerheid als persoonsgegevens moeten behandelen.

Voorbeeld 16: schade door graffiti

Personenvoertuigen in het bezit van een vervoersbedrijf worden herhaaldelijk beschadigd door graffiti. Om de schade te kunnen beoordelen en klachten tegen de daders te kunnen indienen, zet het bedrijf een register op met informatie over de omstandigheden van de schade, met inbegrip van afbeeldingen van de beschadigde voertuigen en de “tags” of “handtekening” van de dader. Wanneer de informatie in het register wordt ingevoerd, zijn de aanbrengers van de graffiti niet bekend, evenmin als de persoon waarmee de “handtekening” correspondeert. Het is heel goed mogelijk dat die personen nooit bekend zullen worden. Het doel van de verwerking is echter juist de identificatie van de personen wie de informatie over de daders betreft, zodat tegen hen een rechtsvordering kan worden ingesteld. Deze verwerking heeft zin als de voor de verwerking verantwoordelijke het “redelijkerwijs waarschijnlijk acht” dat de persoon ooit zal kunnen worden geïdentificeerd. De informatie die in de afbeeldingen is vervat, moet worden beschouwd als informatie betreffende “identificeerbare” personen, de informatie in het register is derhalve een persoonsgegeven en op de verwerking ervan zijn dus de regels inzake gegevensbescherming van toepassing. Die regels staan de verwerking in bepaalde omstandigheden en onder zekere waarborgen toe als rechtmatig.

Als identificatie van de betrokkene niet tot het doel van de verwerking behoort, wordt een zeer belangrijke rol gespeeld door de technische maatregelen die identificatie moeten voorkomen. Het inzetten van geschikte technische en organisatorische maatregelen, volgens de laatste stand van de techniek, om mogelijke identificatie te voorkomen, kan ertoe leiden dat de betrokkenen niet meer identificeerbaar zijn wanneer rekening wordt gehouden met *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* voor de identificatie van de betrokkenen. In dit geval is de tenuitvoerlegging van de bedoelde maatregelen niet het *gevolg* van een wettelijke verplichting die uit artikel 17 van de richtlijn voortvloeit (dat artikel is namelijk van toepassing als de informatie sowieso al als persoonsgegeven geldt), maar veeleer een *voorwaarde* om de informatie niet als persoonsgegeven te kunnen beschouwen, waardoor de verwerking ervan niet aan de richtlijn is onderworpen.

Gepseudonimiseerde gegevens

Pseudonimisering betekent het verhullen van een identiteit. Dit wordt gedaan om aanvullende gegevens over dezelfde persoon te kunnen verzamelen zonder diens identiteit te hoeven kennen. Dit is vooral van belang in de context van onderzoek en statistiek.

Gegevens kunnen zodanig worden gepseudonimiseerd dat de gegevens kunnen worden teruggevoerd tot hun oorsprong door gebruik te maken van ofwel correspondentielijsten van identiteiten en de bijbehorende pseudoniemen, ofwel algoritmen voor tweerichtingsversleuteling. Identiteiten kunnen ook zodanig worden verhuld dat re-identificatie onmogelijk is, bijvoorbeeld door middel van eenrichtingsversleuteling, waardoor over het algemeen geanonimiseerde gegevens ontstaan.

De effectiviteit van de procedure die voor de pseudonimisering wordt toegepast, is afhankelijk van een aantal factoren: in welk stadium de procedure wordt toegepast, hoe sterk de beveiliging tegen herleiding is, de omvang van de populatie waarvan de betrokkene deel uitmaakt, de mogelijkheid om afzonderlijke transacties of records aan dezelfde persoon te koppelen, enz. De pseudoniemen moeten willekeurig en onvoorspelbaar zijn. Het aantal mogelijke pseudoniemen moet zo groot zijn dat nooit meer dan eens hetzelfde pseudoniem wordt gekozen. Is een hoge mate van beveiliging vereist, dan moet het aantal mogelijke pseudoniemen ten minste even groot zijn als het aantal waarden van veilige cryptografische hashfuncties[13].

Herleidbare gepseudonimiseerde gegevens kunnen worden beschouwd als informatie over *indirect identificeerbare* personen. Door gebruik van een pseudoniem kunnen gegevens worden herleid tot de betrokkene, zodat diens identiteit kan worden vastgesteld, maar dit is slechts mogelijk in welbepaalde omstandigheden. In dergelijke gevallen zijn de regels voor gegevensbescherming van toepassing, maar de betrokkenen lopen bij de verwerking van dergelijke indirect identificeerbare informatie meestal slechts een gering risico. De regels worden in die gevallen dan ook soepeler toegepast dan bij de verwerking van informatie over direct identificeerbare personen.

Met een code aangeduide gegevens

Bij het klassieke voorbeeld van pseudonimisering worden gegevens aangeduid met een code. De informatie heeft betrekking op personen die met een code worden aangeduid, terwijl de sleutel die de koppeling vormt tussen de code en de normale identificatiemiddelen van personen (bijvoorbeeld naam, geboortedatum, adres) afzonderlijk wordt bewaard.

Voorbeeld 17: niet-geaggregeerde statistische gegevens

De noodzaak met alle omstandigheden rekening te houden bij de beoordeling of middelen redelijkerwijs kunnen worden ingezet voor identificatie, kan worden geïllustreerd met het volgende voorbeeld: persoonlijke informatie wordt verwerkt door het nationaal bureau voor de statistiek. Daarbij wordt in een bepaald stadium informatie in niet-geaggregeerde vorm bewaard die specifieke personen betreft, maar die personen worden aangeduid met een code in plaats van met hun naam (bijvoorbeeld de persoon met de code X1234 drinkt meer dan driemaal per week een glas wijn). De sleutel tot deze codes (de lijst waarmee kan worden vastgesteld welke naam met welke code overeenstemt) wordt door het bureau voor de statistiek apart bewaard. Die sleutel kan worden gerekend tot de middelen die door het bureau voor de statistiek “redelijkerwijs kunnen worden ingezet”; de informatie betreffende personen kan daarom worden beschouwd als persoonsgegevens en is onderworpen aan de regels voor gegevensbescherming. Stellen we ons nu voor dat een lijst met gegevens over wijnconsumptie

[13] Zie het werkdocument “Datenschutzfreundliche Technologien” (“Privacy-enhancing technologies”) (oktober 1997) van de werkgroep “Datenschutzfreundliche Technologien” van de Arbeitskreis “Technische und organisatorische Datenschutzfragen” van de Duitse commissarissen voor gegevensbescherming op federaal en deelstaatniveau. Het document is te vinden op http://ec.europa.eu/justice_home/fsj/privacy/studies/priv-enhancing_en.htm.

ter beschikking wordt gesteld aan de nationale organisatie van wijnproducenten, zodat deze hun publieke standpunt kunnen staven met statistische gegevens. Om vast te stellen of de lijst met informatie nog steeds als persoonsgegevens geldt, met worden beoordeeld of de afzonderlijke wijndrinkers kunnen worden geïdentificeerd met *"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"*.

Zijn de gebruikte codes uniek voor elke persoon, dan doet het risico van identificatie zich voor als het mogelijk is de encryptiesleutel te achterhalen. Het risico dat de systemen door een buitenstaander worden gekraakt, de waarschijnlijkheid dat iemand binnen de organisatie van de verzender (ondanks het beroepsgeheim) de sleutel ter beschikking stelt *en* de haalbaarheid van indirecte identificatie zijn dus allemaal factoren waarmee rekening moet worden gehouden om te bepalen of de betrokkenen kunnen worden geïdentificeerd *met 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*, en of de informatie dus als "persoonsgegevens" moet worden beschouwd. Is dat het geval, dan zijn de regels inzake gegevensbescherming van toepassing. Een andere kwestie is dat de regels voor gegevensbescherming rekening zouden kunnen houden met de omvang van het risico voor de betrokkenen, en voor de verwerking striktere of minder strikte voorwaarden zouden kunnen stellen overeenkomstig de flexibiliteit die de regels van de richtlijn bieden.

Indien de gebruikte codes echter niet uniek zijn, maar bijvoorbeeld hetzelfde codenummer (laten we zeggen "123") wordt gebruikt om personen in verschillende steden en gegevens voor verschillende jaren aan te duiden (een bepaald individu wordt alleen onderscheiden binnen eenzelfde jaar en binnen de populatie in één stad), kan de voor de verwerking verantwoordelijke, of een derde, een specifieke persoon slechts identificeren indien bekend is op welk jaar en welke stad de gegevens betrekking hebben. Is deze aanvullende informatie onbekend en kan die niet met redelijkerwijs in te zetten middelen worden achterhaald, dan kan de informatie worden beschouwd als informatie die geen identificeerbare personen betreft, en gelden de regels voor gegevensbescherming voor deze informatie niet.

Dit type gegevens wordt vaak gebruikt in de context van klinische proeven met geneesmiddelen. Bij Richtlijn 2001/20/EG van 4 april 2001 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten inzake de toepassing van goede klinische praktijken bij de uitvoering van klinische proeven met geneesmiddelen voor menselijk gebruik[14] wordt een juridisch kader voor deze activiteiten vastgesteld. De onderzoeker die de geneesmiddelen beproeft, verzamelt informatie over de klinische resultaten van elke patiënt en duidt deze aan met een code. De onderzoeker verstrekt deze informatie aan het farmaceutische bedrijf of andere betrokkenen ("opdrachtgevers") uitsluitend in deze gecodeerde vorm, aangezien zij alleen interesse hebben in biostatistische gegevens. De onderzoeker bewaart echter afzonderlijk een sleutel waarmee de code kan worden gekoppeld aan de normale identificatiegegevens van de patiënt. Ter bescherming van de gezondheid van de patiënten wanneer de geneesmiddelen gevaarlijk blijken te zijn, moet de onderzoeker deze sleutel bewaren, zodat de afzonderlijke patiënten zo nodig kunnen worden geïdentificeerd en een passende behandeling kunnen krijgen.

De vraag is hier of de voor de klinische proef gebruikte gegevens kunnen worden geacht gegevens betreffende "identificeerbare" natuurlijke personen te zijn en of dus de regels voor gegevensbescherming erop van toepassing zijn. Zoals eerder gezegd moet, om te bepalen of een persoon identificeerbaar is, worden gekeken naar alle middelen waarvan mag worden

[14] PB L 121 van 1.5.2001, blz. 34.

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. In dit geval is identificatie van de betrokkenen (om hun in geval van nood een passende behandeling te kunnen geven) een van de doeleinden van de verwerking van de met een code aangeduide gegevens. Het farmaceutisch bedrijf heeft de middelen voor de verwerking, met inbegrip van de organisatorische maatregelen, en zijn betrekkingen met de onderzoeker die de sleutel onder zijn hoede heeft, zo opgezet dat identificatie van de betrokkenen niet alleen *kan* gebeuren, maar in bepaalde omstandigheden *moet* gebeuren. De identificatie van de patiënten maakt dus deel uit van het doel en de wijze van de verwerking. De conclusie kan in dit geval luiden dat met een code aangeduide gegevens informatie zijn betreffende identificeerbare natuurlijke personen, en wel voor alle partijen die bij de mogelijke identificatie betrokken zijn, en als zodanig onder de regels voor gegevensbescherming vallen. Dit betekent echter niet dat wanneer een andere voor verwerking verantwoordelijke met dezelfde gegevensverzameling werkt, hij eveneens noodzakelijkerwijs persoonsgegevens verwerkt, op voorwaarde dat die andere voor verwerking verantwoordelijken de verwerking zodanig organiseren dat re-identificatie uitdrukkelijk is uitgesloten en ter voorkoming daarvan passende technische maatregelen zijn genomen.

Op andere onderzoeksterreinen of in andere onderdelen van hetzelfde project kan door de opzet van de protocollen en procedures de re-identificatie van de betrokkenen onmogelijk zijn gemaakt, bijvoorbeeld omdat er geen therapeutische gegevens bij zijn betrokken. Het kan technisch of anderszins nog steeds mogelijk zijn om te achterhalen op welke personen klinische gegevens betrekking hebben, maar identificatie wordt niet verondersteld of verwacht plaats te vinden onder welke omstandigheden dan ook, en om identificatie te voorkomen zijn passende technische maatregelen genomen (bijvoorbeeld encryptie, onomkeerbare hashing). Zelfs als bepaalde betrokkenen in dit geval ondanks al die protocollen en maatregelen kunnen worden geïdentificeerd (door onvoorziene omstandigheden zoals toevallige koppeling met eigenschappen van de betrokkene waaruit zijn/haar identiteit blijkt), kan de informatie die is verwerkt door de oorspronkelijk voor de verwerking verantwoordelijke niet worden geacht betrekking te hebben op personen die geïdentificeerd zijn of identificeerbaar, rekening houdende met *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.* Het kan dus zijn dat de verwerking ervan niet onder de bepalingen van de richtlijn valt. Het is een andere zaak als de nieuwe voor de verwerking verantwoordelijke effectief toegang heeft gekregen tot de identificeerbare informatie. In dat geval is er zonder enige twijfel sprake van persoonsgegevens.

FAQ 14, punt 7, van de Veiligehavenregeling

De kwestie van met codes aangeduide gegevens bij farmaceutisch onderzoek is aan de orde gekomen in het kader van de Veiligehavenregeling[15]. FAQ 14, punt 7, luidt als volgt:

"FAQ 14: Farmaceutische en medische producten

V7: De hoofdonderzoeker voorziet de onderzoeksgegevens altijd van een unieke code naar oorsprong, zodat de identiteit van de individuen waarop de gegevens betrekking hebben geheim blijft. De farmaceutische bedrijven die de opdracht voor het onderzoek hebben gegeven, krijgen niet de beschikking over de sleutel. Deze is uitsluitend bij de onderzoeker bekend, zodat hij onder bepaalde omstandigheden (bv. als nadere medische zorg nodig is) de betrokkene kan identificeren. Is een doorgifte van dusdanig gecodeerde gegevens van de

[15] Beschikking 2000/520/EG van de Commissie van 26.7.2000, PB L 215 van 25.8.2000, blz. 7.

Europese Unie naar de Verenigde Staten een doorgifte van persoonsgegevens waarop de Veiligehavenbeginselen van toepassing zijn?

A: Nee. Dit geldt niet als een doorgifte van persoonsgegevens waarop de beginselen van toepassing zijn."

De Groep meent dat deze uitspraak in het kader van de Veiligehavenregeling niet in strijd is met de hierboven aangevoerde redenering waarbij wordt aanbevolen dergelijke informatie als persoonsgegevens in de zin van de richtlijn te beschouwen. Deze FAQ is namelijk niet precies genoeg, omdat niet wordt aangegeven aan wie en onder welke omstandigheden de gegevens worden doorgegeven. Volgens de Groep heeft de FAQ betrekking op de doorgifte van de met codes aangeduide gegevens aan geadresseerden in de VS (bijvoorbeeld farmaceutische bedrijven), die uitsluitend de gecodeerde gegevens ontvangen en nooit zullen weten wie de patiënten zijn. Hun identiteit is alleen te achterhalen, mocht dat noodzakelijk zijn voor eventuele behandeling, door de arts/onderzoeker in de EU, maar nooit door het Amerikaanse bedrijf.

Anonieme gegevens

"Anonieme gegevens" zoals bedoeld in de richtlijn kunnen worden gedefinieerd als informatie betreffende een natuurlijke persoon die niet kan worden geïdentificeerd, noch door de voor de verwerking verantwoordelijke, noch door een andere persoon, *rekening houdende met 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* voor de identificatie van de betrokkene. "Geanonimiseerde gegevens" zijn dan anonieme gegevens betreffende een persoon die eerder identificeerbaar was, maar nu niet meer kan worden geïdentificeerd. In overweging 26 wordt hierover gesteld *"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"*. De beoordeling of de gegevens identificatie van de betrokkene mogelijk maken en of de informatie als anoniem kan worden beschouwd, is ook in dit geval afhankelijk van de omstandigheden. Per geval moet dit worden bekeken, met name of de voor identificatie redelijkerwijs in te zetten middelen aanwezig zijn zoals omschreven in overweging 26. Dit is met name relevant voor statistische informatie, wanneer de informatie weliswaar wordt gepresenteerd als geaggregeerde gegevens, maar de oorspronkelijke steekproef niet voldoende groot is en andere gegevens identificatie van betrokkenen mogelijk maken.

Voorbeeld 18: Statistisch onderzoek en combinatie van verspreide informatie

Statistici zijn zoals iedereen verplicht de regels voor gegevensbescherming na te leven en te zorgen voor anonimiteit van het statistisch onderzoek, maar er geldt voor hen ook een specifieke professionele geheimhoudingsplicht, op grond waarvan het hun verboden is niet-anonieme gegevens te publiceren. Zij zijn daarom verplicht statistische gegevens in geaggregeerde vorm te publiceren, waardoor ze niet kunnen worden teruggevoerd op geïdentificeerde personen. Deze regel is met name van belang bij de publicatie van volkstellingsgegevens. Voor iedere situatie moet worden vastgesteld onder welke drempelwaarde personen identificeerbaar zijn. Als een criterium ertoe leidt dat iemand kan worden geïdentificeerd binnen een gegeven categorie personen, hoe groot die categorie ook is (bijvoorbeeld in een stad met 6000 inwoners werkt slechts één arts), dan moet dit onderscheidende criterium achterwege blijven en moeten andere criteria worden toegevoegd om de resultaten voor een bepaalde persoon te "verdunnen", zodat het statistische geheim in stand blijft.

Voorbeeld 19: publicatie van videobewakingsbeelden

Een winkelier installeert in zijn zaak een systeem voor camerabewaking. Hij hangt in de zaak foto's op van winkeldieven die met het bewakingssysteem zijn opgenomen. Na een waarschuwing van de politie maakt hij het gezicht van de dieven onherkenbaar. Maar ook dan bestaat nog steeds de mogelijkheid dat de personen op de foto's worden herkend door vrienden, familie of buren aan hun haardracht, lichaamsfiguur of kleding.

4. VIERDE ELEMENT: "NATUURLIJKE PERSOON"

De bescherming die de regels van de richtlijn bieden, geldt voor natuurlijke personen, dat wil zeggen mensen. Het recht op de bescherming van persoonsgegevens is in die zin een universeel recht, dat niet beperkt is tot ingezetenen of onderdanen van een bepaald land. In overweging 2 van de richtlijn wordt dit expliciet gemaakt door te stellen dat *"de systemen voor de verwerking van gegevens ten dienste van de mens staan"* en dat zij *"de fundamentele rechten en vrijheden en inzonderheid de persoonlijke levenssfeer van natuurlijke personen, ongeacht hun nationaliteit of verblijfplaats, moeten eerbiedigen"*.

Het begrip natuurlijke persoon wordt aangehaald in artikel 6 van de Universele Verklaring van de rechten van de mens, waarin wordt gesteld: *"Een ieder heeft, waar hij zich ook bevindt, het recht als persoon erkend te worden voor de wet."* In de wetgeving van de lidstaten, doorgaans in hun burgerlijk recht, wordt het concept van de persoonlijkheid van mensen verder uitgewerkt. Dit wordt opgevat als hun rechtsbekwaamheid, die een aanvang neemt bij de geboorte en eindigt met de dood. Persoonsgegevens zijn derhalve in beginsel gegevens betreffende geïdentificeerde of identificeerbare *levende personen*. Hierdoor worden in dit verband een aantal vragen opgeworpen.

Gegevens betreffende overledenen

Informatie over overleden personen wordt dus in beginsel niet beschouwd als persoonsgegevens waarop de regels van de richtlijn van toepassing zijn, aangezien overledenen civielrechtelijk geen natuurlijke personen meer zijn. Gegevens betreffende overledenen kunnen echter in bepaalde gevallen indirect nog enige bescherming genieten.

Ten eerste is het mogelijk dat degene die voor de gegevensverwerking verantwoordelijk is, niet kan nagaan of de betrokkene nog leeft of inmiddels is overleden. Ook wanneer hij daartoe wel in staat is, kan het zijn dat gegevens over overledenen op dezelfde wijze worden verwerkt als gegevens betreffende levende personen. Aangezien de voor de verwerking verantwoordelijke, wat gegevens over levende personen betreft, volgens de richtlijn onderworpen is aan de verplichting tot bescherming van de gegevens, is het voor hem waarschijnlijk eenvoudiger om gegevens over overledenen eveneens volgens de regels voor gegevensbescherming te verwerken, in plaats van de twee soorten gegevens gescheiden te houden.

Ten tweede kan het zijn dat informatie over overledenen daarnaast ook betrekking heeft op levende personen. Het gegeven dat de overleden Gaia aan hemofilie leed, wijst er bijvoorbeeld op dat haar zoon Titius dezelfde ziekte heeft, aangezien deze wordt doorgegeven door een gen op het X-chromosoom. Wanneer informatie over overledenen dus tegelijkertijd levende personen betreft en daardoor als persoonsgegeven in de zin van de richtlijn geldt, geniet die informatie over een overleden persoon indirect de bescherming die de bepalingen van de richtlijn bieden.

Ten derde kan informatie over overledenen specifieke bescherming genieten op grond van andere regels dan de gegevensbeschermingswetgeving, die de grenzen afbakenen van wat sommigen *"personalitas praeterita"* noemen. De vertrouwelijkheidsplicht van medisch personeel eindigt niet met de dood van de patiënt. De nationale wetgeving inzake het portretrecht en ter bescherming tegen eerroof kan ook de nagedachtenis van de doden in bescherming nemen.

Ten vierde verzet niets zich ertegen dat een lidstaat de draagwijdte van de nationale wettelijke regeling houdende uitvoering van de bepalingen van Richtlijn 95/46/EG uitbreidt tot niet binnen de werkingssfeer daarvan vallende gebieden, voor zover geen enkele andere bepaling van gemeenschapsrecht daaraan in de weg staat, zoals het Hof van Justitie heeft opgemerkt[16]. Het is mogelijk dat een nationale wetgever de bepalingen van de nationale wetgeving inzake gegevensbescherming ook van toepassing verklaart op de verwerking van gegevens betreffende overledenen, indien een rechtmatig belang zulks rechtvaardigt[17].

Ongeboren kinderen

In hoeverre de regels voor gegevensbescherming vóór de geboorte al van toepassing zijn, hangt af van het standpunt dat in de nationale rechtsstelsels wordt ingenomen ten aanzien van de bescherming van ongeboren kinderen. Met name in het erfrecht hanteren sommige lidstaten het beginsel dat verwekte, maar nog niet geboren kinderen als reeds geboren worden beschouwd waar het gaat om het ontvangen van voordelen (en dus een erfenis of schenking kunnen krijgen), mits zij later ook daadwerkelijk geboren worden. In andere lidstaten bieden bepaalde rechtsregels specifieke bescherming, wanneer aan deze zelfde voorwaarde is voldaan. Om te bepalen of de nationale wetgeving inzake gegevensbescherming ook informatie betreffende ongeboren kinderen beschermt, moet rekening worden gehouden met de algemene aanpak die het nationale rechtsstelsel hanteert, en met het feit dat het doel van de regels voor gegevensbescherming is personen te beschermen.

Een tweede vraag wordt opgeworpen door de overweging dat de algemene aanpak van het rechtsstelsel uitgaat van de veronderstelling dat de situatie van ongeboren kinderen beperkt blijft tot de duur van de zwangerschap. Er wordt geen rekening gehouden met de omstandigheid dat deze situatie in feite langer kan duren, bijvoorbeeld waar het gaat om ingevroren embryo's. Tot slot kan een specifieke juridische respons te vinden zijn in bepalingen over voortplantingstechnieken, waarin het gebruik van medische of genetische informatie over embryo's wordt geregeld.

Rechtspersonen

Aangezien in de definitie van persoonsgegevens slechts naar natuurlijke personen wordt verwezen, valt informatie betreffende rechtspersonen in beginsel niet onder de richtlijn en geldt de bescherming die de richtlijn biedt niet voor rechtspersonen[18]. Bepaalde regels inzake gegevensbescherming kunnen echter in bepaalde omstandigheden indirect toch van toepassing zijn op informatie betreffende ondernemingen of rechtspersonen.

---

16 Arrest van het Hof van Justitie in de zaak C-101/2001 van 6.11.2003 (Lindqvist), punt 98.

17 Notulen van de Raad van de Europese Unie van 8.2.1995, document 4730/95: "Ad artikel 2, onder a): *De Raad en de Commissie bevestigen dat de lidstaten kunnen bepalen of en in hoeverre de richtlijn wordt toegepast op overleden personen."*

18 Overweging 24 van de richtlijn: *"Overwegende dat deze richtlijn niet van invloed is op regelingen inzake de bescherming van rechtspersonen in verband met de verwerking van persoonsgegevens die op hen betrekking hebben;"*.

Sommige bepalingen van Richtlijn 2002/58/EG inzake e-privacy gelden ook voor rechtpersonen. In artikel 1 van die richtlijn wordt bepaald: *"2. Voor de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op Richtlijn 95/46/EG. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn."* In de artikelen 12 en 13 wordt de toepassing van sommige bepalingen inzake abonneelijsten en ongewenste communicatie dan ook uitgebreid tot rechtspersonen.

Volgens de criteria die in dit document zijn uiteengezet, kan informatie over rechtspersonen ook op eigen merites worden beschouwd als informatie "betreffende" natuurlijke personen. Dat kan het geval zijn als de naam van de rechtspersoon is afgeleid van de naam van een natuurlijke persoon. Een andere geval kan zich voordoen bij bedrijfs-e-mail, die normaliter wordt gebruikt door een specifieke werknemer, of bij informatie over een klein bedrijf (rechtens eerder een voorwerp dan een rechtspersoon) die ook iets zegt over het gedrag van de eigenaar. Wanneer informatie over een rechtspersoon of een bedrijf op grond van de criteria "inhoud", "doel" of "resultaat" kan worden beschouwd als informatie "betreffende" een natuurlijke persoon, geldt in al deze gevallen dat deze informatie als persoonsgegeven moet worden beschouwd en dat de regels voor gegevensbescherming van toepassing moeten zijn.

Het Hof van Justitie heeft duidelijk gesteld dat niets zich ertegen verzet dat een lidstaat de draagwijdte van de nationale wettelijke regeling houdende uitvoering van de bepalingen van de richtlijn uitbreidt tot niet binnen de werkingssfeer daarvan vallende gebieden, voor zover geen enkele andere bepaling van gemeenschapsrecht daaraan in de weg staat[19]. Sommige lidstaten, zoals Italië, Oostenrijk en Luxemburg, hebben de toepassing van sommige bepalingen van de nationale wetgeving houdende uitvoering van de richtlijn (zoals de bepalingen inzake beveiligingsmaatregelen) dan ook uitgebreid tot de verwerking van gegevens betreffende rechtspersonen.

Zoals ook geldt voor informatie over overleden personen, kunnen praktische overwegingen van de voor de verwerking verantwoordelijke er toe leiden dat de regels voor gegevensbescherming de facto ook worden toegepast op gegevens over rechtspersonen. Wanneer de voor de verwerking verantwoordelijke zonder onderscheid gegevens over zowel natuurlijke personen als rechtspersonen verzamelt en deze gegevens in dezelfde gegevensverzamelingen opneemt, kunnen de mechanismen voor gegevensverwerking en het auditingsysteem zo zijn opgezet dat aan de regels voor gegevensbescherming wordt voldaan. Het is voor degene die voor de verwerking verantwoordelijk is wellicht zelfs eenvoudiger de regels voor gegevensbescherming gewoonweg op alle gegevens in zijn bestanden toe te passen en niet uit te zoeken welke gegevens natuurlijke personen betreffen en welke rechtspersonen.

IV. WAT ALS GEGEVENS NIET ONDER DE DEFINITIE VALLEN?

Zoals we in dit document hebben gezien, kan het in diverse omstandigheden gebeuren dat informatie niet als persoonsgegeven wordt beschouwd. Dat is het geval wanneer het niet gaat om informatie betreffende een persoon, of wanneer de persoon niet als geïdentificeerd of identificeerbaar kan worden beschouwd. Wanneer de verwerkte of te verwerken informatie niet onder het begrip "persoonsgegeven" valt, is de consequentie dat de richtlijn niet van toepassing is, overeenkomstig artikel 3 ervan. Dat betekent echter niet dat personen

[19] Arrest van het Hof van Justitie in de zaak C-101/2001 van 6.11.2003 (Lindqvist), punt 98.

in die bepaalde situatie op geen enkele bescherming kunnen rekenen. Er moet rekening worden gehouden met de hiernavolgende overwegingen.

Wanneer de richtlijn niet van toepassing is, kan het zijn dat de nationale wetgeving inzake gegevensbescherming wel van toepassing is. Artikel 34 preciseert dat de richtlijn gericht is tot de lidstaten. Voor zaken die buiten de werkingssfeer van de richtlijn vallen zijn de lidstaten niet onderworpen aan de verplichtingen die bij de richtlijn worden gesteld, namelijk om de nodige wettelijke en bestuursrechtelijke bepalingen in werking te doen treden om aan de richtlijn te voldoen. Zoals het Hof van Justitie duidelijk heeft gesteld, verzet zich echter niets ertegen dat een lidstaat de draagwijdte van de nationale wettelijke regeling houdende uitvoering van de bepalingen van de richtlijn uitbreidt tot niet binnen de werkingssfeer daarvan vallende gebieden, voor zover geen enkele andere bepaling van gemeenschapsrecht daaraan in de weg staat. Het kan zeer goed zo zijn dat bepaalde situaties waarin geen persoonsgegevens in de zin van de richtlijn worden verwerkt, niettemin onderworpen zijn aan beschermende maatregelen van nationaal recht. Dit kan bijvoorbeeld het geval zijn voor gegevens die met een code worden aangeduid, ongeacht of het daarbij om persoonsgegevens gaat.

Ook wanneer de regels inzake gegevensbescherming niet van toepassing zijn, kunnen bepaalde activiteiten wel degelijk in strijd zijn met artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens, waarin het recht op respect voor het privéleven en het familie- en gezinsleven wordt beschermd, dit gezien de verreikende jurisprudentie van het Europees Hof voor de Rechten van de Mens. Andere wettelijke bepalingen, zoals de wetgeving inzake onrechtmatige daad, het strafrecht of de antidiscriminatiewetgeving, kunnen iemand eveneens bescherming bieden wanneer de regels inzake gegevensbescherming niet van toepassing zijn en iemands rechtmatige belangen op het spel staan.

V. CONCLUSIES

De Groep heeft in dit document richtsnoeren geformuleerd voor de wijze waarop het begrip “persoonsgegeven”, zoals dat voorkomt in Richtlijn 95/46/EG en daarmee samenhangende communautaire wetgeving, moet worden opgevat en in verschillende situaties moet worden toegepast.

Als algemene notie heeft de Groep geconstateerd dat de Europese wetgever de bedoeling had een brede inhoud aan het begrip persoonsgegeven te geven, maar niet zonder er grenzen aan te stellen. Men mag niet vergeten dat het doel van de in de richtlijn vervatte regels is om op het gebied van de verwerking van persoonsgegevens de fundamentele rechten en vrijheden van personen te beschermen, met name het recht op de persoonlijke levenssfeer. Die regels waren daarom bedoeld voor situaties waarin de rechten van personen in gevaar zouden kunnen komen en derhalve moesten worden beschermd. De reikwijdte van de regels voor gegevensbescherming mocht niet te ver worden opgerekt, maar ook moest worden voorkomen dat het begrip persoonsgegevens onterecht zou worden ingeperkt. In de richtlijn wordt daarom de werkingssfeer vastgelegd, worden bepaalde activiteiten daarvan uitgesloten en wordt bij de toepassing van de regels op activiteiten die binnen het toepassingsgebied liggen enige flexibiliteit toegestaan. Voor de totstandkoming van een passend evenwicht bij die toepassing wordt een belangrijke rol gespeeld door de gegevensbeschermingsautoriteiten (zie hoofdstuk II).

De analyse van de Groep gaat uit van de vier voornaamste "bouwstenen" die in de definitie van "persoonsgegeven" kunnen worden onderscheiden: "iedere informatie" "betreffende" "een geïdentificeerde of identificeerbare" "natuurlijke persoon". Deze elementen zijn onderling nauw vervlochten en van elkaar afhankelijk, en zijn in combinatie bepalend voor de vraag of een gegeven als "persoonsgegeven" moet worden beschouwd. De analyse wordt geïllustreerd met voorbeelden uit de praktijk van de Europese nationale gegevensbeschermingsautoriteiten.

- Het eerste element – "iedere informatie" – geeft ervan blijk dat een ruime definitie van het begrip is nagestreefd, waarbij de aard of de inhoud van de informatie en de technische vorm ervan geen rol spelen. Dit betekent dat zowel objectieve als subjectieve informatie over een persoon, in welke hoedanigheid ook, als persoonsgegeven kan worden beschouwd, ongeacht het technische medium waarin die informatie is vervat. In het advies wordt ook aandacht besteed aan biometrische gegevens en aan het juridische onderscheid met monsters van menselijk weefsel waarvan die gegevens kunnen worden afgeleid (zie hoofdstuk III, punt 1).

- Het tweede element – "betreffende" – is tot dusver vaak over het hoofd gezien. Het speelt echter een cruciale rol voor het bepalen van de inhoudelijke reikwijdte van het begrip, met name met betrekking tot voorwerpen en nieuwe technologieën. Het advies onderscheidt drie alternatieve aspecten – "inhoud", "doel" en "resultaat" – aan de hand waarvan wordt bepaald of informatie een persoon "betreft". Dit dekt tevens informatie die een duidelijk gevolg kan hebben voor de wijze waarop iemand wordt behandeld of beoordeeld (zie hoofdstuk III, punt 2).

- Bij het derde element – "geïdentificeerd of identificeerbaar" – gaat het met name om de voorwaarden waarop een persoon als "identificeerbaar" kan worden beschouwd, en wordt vooral aandacht besteed aan de "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". De specifieke context en omstandigheden van een geval spelen bij die analyse een belangrijke rol. Het advies gaat ook in op gepseudonimiseerde gegevens en op het gebruik van met een code aangeduide gegeven bij statistisch of farmaceutisch onderzoek (zie hoofdstuk III, punt 3).

- Bij het vierde element – "natuurlijke persoon" – wordt ingegaan op het vereiste dat "persoonsgegevens" levende personen dienen te betreffen. In het advies worden raakvlakken besproken met gegevens over overledenen, ongeboren kinderen en rechtspersonen (zie hoofdstuk III, punt 4).

Het advies bespreekt tot slot wat er gebeurt als gegevens buiten de reikwijdte van de definitie van "persoonsgegeven" vallen. Er kunnen voor dergelijke gevallen verschillende oplossingen voorhanden zijn, waaronder nationale wetgeving met een breder toepassingsgebied dan dat van de richtlijn, mits andere communautaire wetgeving zich daar niet tegen verzet (zie hoofdstuk IV).

De Groep verzoekt alle belanghebbenden de richtsnoeren in dit advies zorgvuldig te bestuderen en ermee rekening te houden bij de interpretatie en de toepassing van de nationale wetgeving overeenkomstig Richtlijn 95/46/EG.

De leden van de Groep, voor het merendeel vertegenwoordigers van toezichthoudende gegevensbeschermingsautoriteiten in de lidstaten, hebben het vaste voornemen de in dit advies gegeven richtsnoeren verder uit te werken in hun eigen rechtsgebied om zo een correcte toepassing van hun nationaal recht overeenkomstig Richtlijn 95/46/EG te bevorderen.

De Groep is voornemens de in dit advies vervatte richtsnoeren toe te passen en waar nodig verder te ontwikkelen. Zij zal er terdege rekening mee houden bij haar verdere werkzaamheden, met name waar het gaat om onderwerpen als identiteitsbeheer in de context van e-overheid en e-gezondheidszorg, alsmede in verband met RFID. Wat RFID betreft, wil de Groep bijdragen tot verder onderzoek naar de mogelijke consequenties van de regels inzake gegevensbescherming voor het gebruik van RFID-tags en de eventuele noodzaak aanvullende maatregelen te nemen om in dat verband te zorgen voor de eerbiediging van rechten en belangen op het gebied van gegevensbescherming.

Tot slot nodigt de Groep alle belanghebbenden en toezichthoudende autoriteiten uit feedback te geven over hun praktische ervaring met de in dit advies vervatte richtsnoeren, geïllustreerd met voorbeelden ter aanvulling op de voorbeelden in dit document. Het is de bedoeling van de Groep te zijner tijd op dit onderwerp terug te komen, om het algemene inzicht in het cruciale begrip persoonsgegeven te versterken. Zij wil zo bevorderen dat Richtlijn 95/46/EG en daarmee samenhangende communautaire wetgeving geharmoniseerd wordt toegepast en beter ten uitvoer wordt gelegd.

Voor de Groep

De voorzitter
Peter Schaar