I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming over de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende radiofrequentie-identificatie (RFID) in Europa: Maatregelen met het oog op een beleidskader COM(2007) 96

(2008/C 101/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 286,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 8,

Gelet op Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens,

Gelet op Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie,

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, en met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. **INLEIDING**

1. Op 15 maart 2007 heeft de Commissie een Mededeling aangenomen, genaamd „Radiofrequentie-identificatie (RFID) in Europa: maatregelen met het oog op een beleidskader" ([1]) (hierna „de Mededeling"). Ingevolge artikel 41 van Verordening (EG) nr. 45/2001 is de EDPS belast met het verstrekken van advies aan de communautaire instellingen en organen in verband met alle aangelegenheden betreffende de verwerking van persoonsgegevens. Overeenkomstig dit artikel presenteert de EDPS presenteert dit advies.

2. Dit advies moet worden gezien als een reactie van de EDPS op de Mededeling en op andere acties op het gebied van RFID sinds de aanneming van de Mededeling. Tot deze andere acties die in dit advies aan bod komen, behoren:

— het besluit van de Commissie van 28 juni 2007 tot oprichting van de Deskundigengroep inzake radiofrequentie-identificatie ([2]), als rechtstreeks gevolg van de Mededeling. Deze groep is ook bekend als de Groep RFID-stakeholders. Overeenkomstig artikel 4, lid 4, onder b) van het besluit neemt de EDPS als waarnemer deel aan de activiteiten van de groep;

— de resolutie van de Raad van 22 maart 2007 over een strategie voor een veilige informatiemaatschappij in Europa ([3]);

— het project „RFID en identiteitsbeheer", een initiatief van het Europees Parlement ([4]);

([1]) COM(2007) 96 def.
([2]) Besluit nr. 467/2007/EG (PB L 176 van 6.7.2007, blz. 25).
([3]) PB C 68 van 24.3.2007, blz. 1.
([4]) Project „RFID and identity management — Case studies from the frontline of the development towards ambient intelligence", in opdracht van de dienst voor de Beoordeling van het wetenschappelijk en technologisch beleid (STOA) van het Europees Parlement, uitgevoerd door de ETAG (*European Technology Assessment Group*) http://www.europarl.europa.eu/stoa/default_en.htm

— de aanneming van advies nr. 4/2007 over het begrip persoonsgegevens door de Groep gegevensbescherming („Groep van artikel 29"), in juni 2007 ([1]);

— de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming ([2]), en het advies van de EDPS over deze mededeling van 25 juli 2007 ([3]);

— de aanneming door de Commissie van een voorstel voor een richtlijn tot wijziging van (onder meer) Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ([4]).

3. De EDPS is blij met de Mededeling van de Commissie over RFID omdat in die mededeling de belangrijkste vraagstukken worden behandeld die zich voordoen in de context van het gebruik van de RFID-technologie, zonder dat wordt voorbijgegaan aan essentiële vragen inzake persoonlijke levenssfeer en gegevensbescherming. Deze mededeling heeft baat gehad bij een consequente en strakke voorbereiding. Voordat de mededeling het daglicht aanschouwde, hebben er namelijk vijf thematische studiebijeenkomsten plaatsgevonden en is er, in opdracht van de Commissie, on-line een openbaar debat ([5]) gehouden.

4. De EDPS is het eens met het standpunt dat RFID-systemen een belangrijke rol zouden kunnen spelen in de ontwikkeling van de informatiemaatschappij ook wel het „internet van dingen" genaamd, en hij deelt ook ten volle de bezwaren in punt 3.2 van de Mededeling, waar staat dat RFID-systemen een bedreiging kunnen vormen voor ieders recht op bescherming van de persoonlijke levenssfeer en van gegevens. In zijn verslag over het jaar 2005 heeft de EDPS RFID-systemen, tezamen met biometrie, intelligente omgeving en systemen voor identiteitsbeheer, genoemd als technologische ontwikkelingen die naar verwachting een zeer grote invloed zullen hebben op gegevensbescherming.

5. Volgens de EDPS zullen de inburgering en de algemene aanvaarding van RFID-technologieën niet alleen worden bereikt door het aantrekkelijke gemak ervan of de nieuwe diensten die zij bieden, maar ook worden bespoedigd dank zij aangepaste en consistente garanties voor gegevensbescherming.

6. Kortom, de EDPS ziet RFID als een ten gronde nieuwe technologische ontwikkeling, die de Commissie in haar Mededeling terecht bestempelt als de poort naar een nieuwe ontwikkelingsfase van de informatiemaatschappij.

7. Deze ontwikkeling doet belangrijke vragen rijzen op allerlei gebieden, zoals dat van gegevensbescherming en de persoonlijke levenssfeer. Dit advies van de EDPS beperkt zich tot laatstgenoemd gebied.

II. INSTEEK VAN HET ADVIES

8. Dit advies neemt vooral als insteek de mogelijke gevolgen van deze ontwikkelingen voor gegevensbescherming en de persoonlijke levensfeer. Het is nu nog onzeker wat deze gevolgen zullen zijn, ook omdat de ontwikkeling en inburgering van RFID-systemen nog volop aan de gang zijn en dat het volkomen onduidelijk is hoever ze zullen gaan.

9. In dat verband volgt de EDPS onderstaande aanpak:

— ten eerste moet duidelijk worden gemaakt wat het gebruik van RFID-systemen voor praktische gevolgen zal hebben voor gegevensbescherming en de persoonlijke levenssfeer;

— ten tweede moeten deze gevolgen worden gespecificeerd, binnen het bestaande rechtskader voor gegevensbescherming en de persoonlijke levenssfeer;

— ten derde roert de EDPS de vraag aan of deze gevolgen specifiekere voorschriften vereisen om vraagstukken inzake gegevensbescherming die voortvloeien uit het gebruik van RFID-technologieën, aan te pakken. Dit punt is door de EDPS reeds aan de orde gesteld in zijn advies inzake de mededeling over de richtlijn gegevensbescherming en zal in dit advies verder worden uitgewerkt.

10. Met deze aanpak hoopt de EDPS te bereiken dat bij de ontwikkeling en de inburgering van RFID-systemen niet voorbij zal worden gegaan aan de gerechtvaardigde bezorgdheid over gegevensbescherming en de persoonlijke levenssfeer.

III. DE GEVOLGEN DUIDELIJK MAKEN

RFID-systemen en -tags

11. Ondanks het feit dat, zoals gezegd, de ontwikkelingen in volle gang zijn en niet bekend is waar ze toe zullen leiden, is het heel goed mogelijk de belangrijkste kenmerken te beschrijven met het oog op de gevolgen voor de gegevensbescherming.

([1]) Document WP 136, dat op de website van de groep staat.
([2]) Mededeling van de Commissie van 7 maart 2007 aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming (COM(2007) 87 def.).
([3]) PB C 255 van 27.10.2007, blz. 1. Hierna: „Advies inzake de mededeling over de richtlijn gegevensbescherming".
([4]) Voorstel van 13 november 2007 voor een richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten; Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking met betrekking tot consumentenbescherming (COM(2007) 698 def.). Richtlijn 2002/58/EG wordt verder geciteerd als de „e-privacy-richtlijn".
([5]) http://www.rfidconsultation.eu/

12. Bij het beoordelen van de mogelijke aspecten qua gegevensbescherming en persoonlijke levenssfeer van de RFID-technologie moet er zeker niet alleen worden gekeken naar de RFID-tags, maar naar de gehele RFID-infrastructuur: de tag, de leesapparatuur, het netwerk, de referentiegegevensbank en de gegevensbank waarin de gegevens die door de combinatie tag/leesapparatuur worden voortgebracht, worden opgeslagen. Zoals in de inleiding tot de Mededeling kort wordt gesteld, is RFID niet gewoon een „elektronische tag". En dus blijven vraagstukken inzake gegevensbescherming niet beperkt tot tags, maar beslaan zijn alle delen van de RFID-infrastructuur. Elk van deze onderdelen levert namelijk een bijdrage aan de uitvoering van het Europese rechtskader voor gegevensbescherming, indien nodig. Zij worden gevoed door de belangrijkste tendensen in de zich ontwikkelende informatiemaatschappij, zoals een bijna onbeperkte bandbreedte, alom tegenwoordige netwerkaansluitingen en een eindeloze opslagcapaciteit.

Invloed van RFID-systemen en -tags

13. Hoewel eerder is gesteld dat een bredere aanpak noodzakelijk is, zijn er verscheidene redenen om allereerst de aandacht te richten op het gebruik van RFID voor tags op consumentenproducten, onder meer in de detailhandel. De meest voor de hand liggende reden is het verwachte toenemende gebruik ervan, dat in de richting lijkt te gaan van een wijdverspreide toepassing. In tegenstelling tot andere RFID-toepassingen met een eng of beperkt gebruik, zou een tag per product wel eens massaal op de markt toegepast kunnen worden. Reeds nu zit aan veel consumentenproducten een RFID-tag. Daaraan gekoppeld is er het feit dat zo'n gebruik een enorm aantal mensen zal betreffen wier persoonsgegevens iedere keer dat zij een product aanschaffen waaraan een RFID-tag zit, worden verwerkt.

14. Er moet specifiek aandacht worden geschonken aan de gevolgen van RFID-tags voor de eigenaars van producten. RFID-systemen zouden een verband kunnen leggen tussen een product en de eigenaar ervan. Zodra dat verband is gelegd, kan de eigenaar worden gescand en ingedeeld als „laag budget" of „aantrekkelijk doel" voor toekomstige transacties. Indien er te veel één-op-één ([1]) wordt toegewezen, kan dat leiden tot automatische „bestraffing" van een bepaald bedrag (recycleringsverplichting, afval, enz.). Mensen mogen niet te maken krijgen met tegen hen gerichte automatische besluiten. Door deze RFID-mogelijkheid neemt het gevaar toe dat de informatiemaatschappij evolueert naar een situatie waarin automatische besluiten worden genomen en waarin de technologie wordt misbruikt om het menselijk gedrag te sturen.

15. De gegevens in, of geproduceerd door een RFID-tag, kunnen persoonsgegevens zijn in de zin van artikel 2 van de richtlijn gegevensbescherming. Smartcards die voor reizen worden gebruikt kunnen bijv. identificatiegegevens bevatten en gegevens over de recente reizen van de houder. Indien een gewetenloos iemand mensen wil volgen, hoeft hij alleen maar op strategische locaties afleesapparatuur te plaatsen, die hem informatie zal geven over de bewegingen van de kaarthouders, waardoor hun persoonlijke levenssfeer en persoonsgegevens worden geschonden.

16. Gelijkaardige bedreigingen van de persoonlijke levenssfeer kunnen zich zelfs voordoen indien de RFID-tag geen namen van personen bevat. Op RFID-tags staan unieke identificaties van consumentenproducten: indien iedere tag een unieke identificatie heeft, kan die identificatie worden gebruikt om iemand te observeren. Indien iemand bijvoorbeeld een horloge draagt waarin een RFID-tag zit met een ID-nummer, kan dat ook dienen als een unieke identificeerder voor de drager van het horloge, zelfs indien diens identiteit onbekend is. Afhankelijk van de wijze waarop de informatie wordt gebruikt en in verband wordt gebracht met het horloge of de persoon, kan de richtlijn wel of niet gelden. De richtlijn geldt bijvoorbeeld als informatie wordt gegenereerd over de verblijfplaats van personen die waarschijnlijk wordt gebruikt om hun gedrag te observeren, of bijvoorbeeld voor prijsdifferentiatie, het ontzeggen van toegang of ongewenste reclame.

17. In dit verband moet ervoor worden gezorgd dat RFID-toepassingen worden omgeven met de nodige technologische maatregelen om het gevaar van ongewilde vrijgave van informatie zo klein mogelijk te houden. Zulke maatregelen kunnen inhouden dat wordt geëist dat de RFID-infrastructuur, vooral RFID-tags, zodanig wordt ontworpen dat dit gevaar wordt voorkomen. RFID-tags zouden kunnen worden voorzien van een „uitschakelbevel" waardoor ze worden gedeactiveerd. Dit zal verder worden besproken in hoofdstuk IV van dit advies.

18. RFID-systemen bieden nieuwe mogelijkheden om producten na het verkooppunt te volgen, en dat levert nieuwe onderwerpen op in het debat over de persoonlijke levenssfeer. Bij de analyse van de gevolgen moet worden gekeken naar twee dingen: in hoeverre wordt het product beschouwd als iets persoonlijks en hoe mobiel is het ([2])?

19. De levenscyclus van een voorwerp kan een aanvulling zijn op de vereiste risicoanalyse en kan bijdragen aan de kwantitatieve beoordeling van de potentiële bedreigingen van de persoonlijke levenssfeer. Gelet op het feit dat een tag misschien niet wordt gedeactiveerd, kan een eindgebruikersproduct met een lange levenscyclus meer gegevens van de eigenaar van het product vergaren en een nauwkeuriger profiel opbouwen. Aan de andere kant zal een product met een korte levenscyclus, zoals een blikje frisdrank, vanaf de productie tot aan de recyclage wellicht minder gevaren opleveren en dus lichtere maatregelen vereisen dan een product met een veel langere levenscyclus.

([1]) Dr. Sarah Spiekermann, director *Berlin Research Centre on Internet Economics, workshop on RFID and ubiquitous computing organized by the Trans Atlantic Consumer Dialogue, 13 March 2007.*

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, *Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No. 2/2007.*

Vraagstukken i.v.m. de persoonlijke levenssfeer en gegevensbescherming bij het gebruik van RFID

20. Voor een beter begrip van de gevolgen van RFID-systemen voor de persoonlijke levenssfeer en gegevensbescherming, kunnen vijf basispunten van privacy en beveiliging worden onderscheiden.

21. Ten eerste, de identificatie van de betrokkene. Meer dan zestig jaar geleden was de RFID-tag bedoeld om te bepalen of er een vriend of vijand aankwam. Vandaag de dag kunnen RFID-systemen niet alleen de algemene elementen van een voorwerp identificeren maar uiteindelijk ook leiden tot de identificatie van een persoon, en daarom moeten ze dat doen op een manier die gegevensbeschermingsvriendelijk is.

22. Ten tweede, de identificatie van de voor de verwerking verantwoordelijke(n). Met RFID-systemen kan de identificatie van de voor de verwerking verantwoordelijke, zoals omschreven in artikel 2, onder d), van de richtlijn gegevensbescherming, wel eens moeilijker zijn en daarom moet dat punt nader worden bekeken. Het identificeren van de voor de verwerking verantwoordelijke blijft echter een kritische fase in het vaststellen van de verantwoordelijkheden van elk van de actoren die moeten voldoen aan het rechtskader voor de gegevensbescherming. Gedurende de levenscyclus van een tag zou de voor de gegevensverwerking verantwoordelijke verscheidene malen kunnen veranderen op basis van de bijkomende diensten die kunnen worden geleverd met betrekking tot het voorwerp waaraan de tag bevestigd zit.

23. Ten derde, het afgenomen belang van het traditionele onderscheid tussen de persoonlijke en de openbare levenssfeer. Hoewel het onderscheid tussen privé en openbare ruimtes ook in het verleden niet altijd even duidelijk was, zijn de meeste mensen zich bewust van de grenzen tussen beide (en van de grijze zones) en nemen zij een onderbouwd dan wel intuïtief besluit over hoe zij zich moeten opstellen. Volgens Hall [1] wordt privéruimte meestal opgevat als de fysieke afstand tot anderen. Het beheer van de persoonlijke levenssfeer kan ook worden gezien als een dynamisch proces van afbakening van de grens van deze levenssfeer [2]. Daarom is het niet verrassend dat de draadloze aard van tagcommunicatie en het vermogen ervan om buiten het gezichtsveld gegevens te lezen, vraagstukken omtrent de persoonlijke levenssfeer oproept omdat deze traditionele grenzen en het beheer ervan worden vervaagd. Er bestaat namelijk de angst dat het individu geheel of gedeeltelijk de greep op het afstandbeheer die hij tot nog toe had kan verliezen. Zo is de afstand waarover de eerste RFID-systemen gegevens konden lezen zowel door voor- als tegenstanders onder de loep genomen.

24. Ten vierde zijn er de omvang en de fysieke eigenschappen van RFID-tags. Omdat de tag klein en goedkoop moet zijn, zullen de beveiligingsmaatregelen aan dit element van het RFID-systeem per definitie beperkt zijn. Maar het draadloze aspect van de communicatie voegt ook een reeks gevaren toe in vergelijking met communicatie via kabel en dus moeten er extra beveiligingseisen worden gesteld.

25. Ten vijfde, het gebrek aan doorzichtigheid van de verwerking. RFID-systemen kunnen leiden tot ongemerkte verzameling en verwerking van gegevens die gebruikt kunnen worden om een profiel van iemand op te stellen. Dit gevolg kan goed worden geïllustreerd middels een vergelijking van RFID-systemen met de GSM, een vergelijking die wel vaker wordt gemaakt. Enerzijds werd de GSM qua technologie goed aanvaard, onafhankelijk van mogelijke risico's op schending van de persoonlijke levenssfeer. Men zou daaruit kunnen opmaken dat RFID op dezelfde wijze zal worden aanvaard. Anderzijds moet worden benadrukt dat een GSM een zichtbaar voorwerp is dat de eindgebruiker nog in de hand heeft omdat de GSM kan worden uitgezet. RFID kan niet worden uitgezet.

26. Hoewel de eerder genoemde ongemerkte verzameling en verwerking van gegeven wettig kan zijn, is het ook mogelijk en in meerdere omstandigheden zelfs vrij waarschijnlijk dat zulke gegevens op onwettige wijze worden verzameld en verwerkt.

27. De verduidelijkingen in dit hoofdstuk leiden tot de hierna volgende slotsom. Het wijdverbreide gebruik van RFID-technologie is fundamenteel nieuw en kan een fundamentele invloed hebben op onze samenleving en op de bescherming van grondrechten in die samenleving, zoals de persoonlijke levenssfeer en gegevensbescherming. RFID kan een kwalitatieve verandering teweegbrengen.

IV. DE GEVOLGEN SPECIFICEREN

Inleiding

28. Dit hoofdstuk gaat vooral over de invloed van RFID op de bescherming van de grondrechten in onze samenleving, zoals de persoonlijke levenssfeer en gegevensbescherming Dit gebeurt in twee stappen. De eerste is een korte beschrijving van de manier waarop deze grondrechten krachtens het huidige rechtskader worden beschermd. Als tweede stap gaat de EDPS verder in op de mogelijkheden om het huidige rechtskader ten volle te benutten. Deze aspiratie is in het advies over de Mededeling over de richtlijn gegevensbescherming als volgt geïntroduceerd: „Eerst moeten de huidige bepalingen van de richtlijn volledig worden toegepast".

29. Dit is het uitgangspunt: nieuwe technologische ontwikkelingen zoals RFID-systemen hebben een duidelijke invloed op de eisen voor een doeltreffende rechtskader voor gegevensbescherming. Ook kan de noodzaak van doeltreffende bescherming van de persoonsgegevens van een individu beperkingen opleggen voor het gebruik van die nieuwe technologieën. De interactie vindt derhalve in twee richtingen plaats: de technologie beïnvloedt de wetgeving en de wetgeving beïnvloedt de technologie [3].

[1] Hall, E.T.1966, *The Hidden Dimension* (1st ed.), Garden City, N.Y: Doubleday.

[2] Altman, I. 1975, *The Environment and Social Behaviour,* Brooks/Cole Monterrey.

[3] Zie het commentaar van de EDPS van maart 2006 op de mededeling van de Commissie over de interoperabiliteit van Europese gegevensbanken, gepubliceerd op de website van de EDPS.

Bescherming van grondrechten

30. De bescherming van de grondrechten op persoonlijke levenssfeer en gegevensbescherming binnen de Europese Unie wordt in de eerste plaats gegarandeerd door een wetgevingskader, dat nodig is omdat we te maken hebben met rechten die erkend worden in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Het wetgevingskader voor gegevensbescherming en RFID bestaat in beginsel in Richtlijn 95/46/EG over gegevensbescherming en de e-privacy-richtlijn 2002/58/EG ([1]).

31. Het algemene wetgevingskader voor gegevensbescherming, zoals neergelegd in Richtlijn 95/46/EG, geldt voor RFID, voor zover door RFID-systemen verwerkte gegevens vallen onder de definitie van persoonsgegevens. In bepaalde gevallen zijn het duidelijk persoonsgegevens die door de RFID-toepassingen worden verwerkt en vallen deze zonder twijfel onder de richtlijn gegevensbescherming, maar er zijn ook toepassingen waarbij het niet zo vanzelfsprekend is dat de gegevensbeschermingsrichtlijn geldt. In advies nr. 4/2007 van de Groep gegevensbescherming („Groep van artikel 29") over het concept persoonsgegevens wordt getracht een duidelijker en algemeen erkende definitie van het concept persoonsgegevens te geven en zo deze onzekerheid gedeeltelijk weg te nemen ([2]).

32. De situatie wat betreft de e-privacy-richtlijn ligt als volgt: tot nu toe is het niet duidelijk of deze richtlijn van toepassing is op RFID-toepassingen. Daarom staat in het voorstel van de Commissie van 13 november 2007 tot wijziging van de richtlijn een bepaling waarmee wordt beoogd te specificeren dat de richtlijn inderdaad geldt voor bepaalde RFID-toepassingen. Andere RFID-toepassingen vallen wellicht niet onder de richtlijn omdat de richtlijn beperkt is tot de verwerking van persoonsgegevens in verband met het leveren van openbare elektronischecommunicatiediensten van openbare communicatienetwerken.

33. De bescherming van persoonsgegevens kan worden aangevuld met een reeks zelfreguleringsinstrumenten (niet-wetgevend kader). Het gebruik van deze instrumenten wordt in beide richtlijnen actief gestimuleerd, vooral in artikel 27 van de richtlijn gegevensbescherming waarin staat dat de lidstaten en de Commissie de opstelling aanmoedigen van gedragscodes, die bestemd zijn om bij te dragen tot een goede uitvoering van de richtlijn. Zelfreguleringsinstrumenten kunnen bovendien een goede bijdrage leveren aan de uitvoering van de beveiligingsmaatregelen die worden vereist in artikel 17 van de richtlijn gegevensbescherming en artikel 14 van de e-privacy-richtlijn.

([1]) Punt 59 van dit advies gaat over de relevantie van een derde richtlijn, namelijk Richtlijn 1999/5/EG van het Europees Parlement en de Raad van 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit (PB L 91 van 7.4.1999, blz. 10).

([2]) Zie onder meer punt 10 van het advies, genoemd in voetnoot 5.

Volledige uitvoering van het bestaande kader

34. In het advies inzake de Mededeling over de richtlijn gegevensbescherming staat een lijst van de instrumenten die beschikbaar zijn voor een betere uitvoering van de richtlijn. De meeste van de niet-bindende instrumenten van dat advies zijn relevant voor RFID, zoals interpretatiemededelingen of andere communicatie, bevordering van beste praktijken, privacyzegels of privacy-audits door derden In hoofdstuk V wordt de mogelijkheid besproken van het aannemen van specifieke regels voor RFID. Ook binnen het bestaande kader zijn evenwel verbeteringen mogelijk.

Zelfreguleringsinstrumenten

35. De EDPS is het met de Commissie eens dat in een eerste fase ruimte moet worden geboden voor zelfregulering, zodat belanghebbenden snel een omgeving tot stand kunnen brengen die voldoet aan de wet en zo kunnen bijdragen aan de verwezenlijking van een veiliger juridische omgeving.

36. De Commissie zal dit proces van zelfregulering naar verwachting stimuleren en aansturen, in overleg met de Groep RFID-belanghebbenden. In dit verband is de EDPS blij met de in de Mededeling aangekondigde Aanbeveling die naar verwachting specifieke richtsnoeren zal bevatten waarin de „beginselen worden vastgesteld die overheidsdiensten en andere belanghebbenden moeten toepassen ten aanzien van het gebruik van RFID".

37. Volgens de Mededeling zal de zelfregulering de vorm aannemen van een gedragscode of een code van goede praktijken. Afgezien van de vormkwestie, moet volgens de EDPS zelfregulering:

— concrete en praktische adviezen geven over specifieke RFID-toepassingen en zo bijdragen aan de naleving van het rechtskader inzake gegevensbescherming;

— een oplossing bieden voor de specifieke gegevensbeschermingsvraagstukken en -problemen die zich voordoen in de context van algemene RFID-toepassingen;

— bijdragen aan de eenvormige en geharmoniseerde toepassing van de richtlijn gegevensbescherming in de gehele EU, zeker in een sector die waarschijnlijk in de gehele EU dezelfde soort RFID-toepassingen gaat gebruiken;

— door alle belanghebbenden worden toegepast. Niet-naleving moet negatieve (en mogelijkerwijs financiële) gevolgen hebben.

38. De EDPS wijst op één punt waar zelfregulering in het bijzonder nuttig zal zijn. Voor de RFID-toepassingen die met zich meebrengen dat er persoonsgegevens worden verwerkt, legt de gegevensbeschermingsrichtlijn de voor de verwerking verantwoordelijken een aantal verplichtingen op, in het bijzonder in artikel 17 (Beveiliging van de verwerking) en artikel 7 (gegevens worden uitsluitend verwerkt als er passende wettige gronden zijn). Volgens deze bepalingen moeten de voor de verwerking verantwoordelijken enerzijds maatregelen nemen tegen de ongeoorloofde verstrekking van gegevens. Anderzijds moeten zij ervoor zorgen dat de verwerking, zoals vrijgave van de gegevens middels afleesapparatuur, waar nodig, alleen plaatsvindt met kennis van zaken na toestemming van de persoon op wie de gegevens betrekking hebben.

39. Deze bepalingen van de gegevensbeschermingsrichtlijn kunnen worden uitgelegd als een eis dat RFID-toepassingen moeten worden gebruikt met de nodige technische oplossingen die de risico's op ongewenste vrijgave voorkomen of minimaliseren, en die ervoor zorgen dat de verwerking of de overdracht van gegevens alleen geschiedt met kennis van zaken na toestemming, waar nodig. Volgens de EDPS worden het bestaan van zo'n verplichting (om te zorgen voor de nodige technische oplossingen die de risico's op ongewenste vrijgave voorkomen of minimaliseren) en het bindende karakter ervan voor gebruikers van RFID-toepassingen, nog sterker en duidelijker indien deze eis wordt opgenomen in de toekomstige gedragscode of code van goede praktijken waarvan al eerder sprake was. Om al deze redenen beveelt de EDPS krachtig aan om in de Aanbeveling van de Commissie zo'n uitleg van de gegevensbeschermingsrichtlijn op te nemen, en er met nadruk op te wijzen dat er een verplichting bestaat om de RFID-toepassingen te gebruiken met de nodige technologische maatregelen die moeten voorkomen dat gegevens zonder toestemming worden verzameld of vrijgegeven.

Behoefte aan sturing

40. De EDPS beveelt de Commissie aan om, in nauwe samenwerking met de RFID-deskundigengroep, een of meer documenten op te stellen met duidelijke sturing over hoe het huidige rechtskader moet worden toegepast op de RFID-omgeving. De sturing moet praktische manieren aangeven om de beginselen in de gegevensbeschermingsrichtlijn en de e-privacy-richtlijn uit te voeren. Voor de algemene aanpak van de sturing en de concrete inhoud ervan, doet de EDPS de hierna volgende suggesties.

41. Richtsnoeren met beginselen die gelden voor het gebruik van RFID moeten voldoende doelgericht zijn en een sectorspecifieke aanpak volgen. Een standaard aanpak beantwoordt niet aan het nagestreefde doel, namelijk zorgen voor een duidelijk en samenhangend kader. De sturing moet juist beperkt blijven tot goed gedefinieerde sectorale RFID-toepassingen.

42. Voorts moeten de richtsnoeren praktische en doeltreffende methodes voorstellen voor het ontwikkelen van *technieken en normen* die ertoe kunnen bijdragen dat de RFID-systemen stroken met het rechtskader gegevensbescherming en die zullen leiden tot het gebruik van „privacy-by-design".

43. Bij het toepassen van het huidige rechtskader op de RFID-omgeving moet bijzondere aandacht worden besteed aan de naleving van beginselen inzake gegevensbescherming en de verplichtingen die rusten op de voor verwerking verantwoordelijken van RFID-toepassingen. Onderstaande verplichtingen en beginselen zijn van bijzonder belang:

— het beginsel van het recht op informatie, inclusief het recht om te weten wanneer gegevens met afleesapparatuur worden verzameld, en om te weten dat er tags aan producten zijn bevestigd;

— het begrip „toestemming" als een van de rechtsgronden voor de verwerking van gegevens. Dit begrip komt tot uiting in de verplichting om RFID-tags op het verkooppunt te desactiveren, tenzij de betrokkene toestemming heeft gegeven ([1]). Het recht om de RFID-tags te desactiveren dient ook de beoogde beveiliging van de informatie, inhoudende dat ervoor wordt gezorgd dat gegevens die door RFID-tags worden verwerkt niet aan ongewenste derden worden vrijgegeven;

— het recht van personen om niet te maken te krijgen met tegen hen gerichte beslissingen die uitsluitend zijn gebaseerd op de geautomatiseerde verwerking van een welomschreven persoonsprofiel.

44. Wat betreft het recht op informatie, moet in de richtsnoeren worden gesteld dat personen *informatie* moeten krijgen over de verwerking van hun persoonsgegevens. Zij moeten in het bijzonder worden geattendeerd op, onder meer: i) de aanwezigheid van afleesapparatuur en de aanwezigheid van geactiveerde RFID-tags op producten of verpakking; ii) de gevolgen die dit heeft in termen van gegevensverzameling; en iii) het beoogde gebruik van de verzamelde informatie.

45. Het gebruik van logo's kan een goede manier zijn om informatie te geven. Logo's kunnen worden gebruikt om te wijzen op de aanwezigheid van RFID-tags die verondersteld worden actief te blijven. Maar het gebruik van logo's alleen zal niet voldoende zijn om te zorgen voor een eerlijke verwerking van informatie, want daarvoor moet duidelijke en begrijpelijke informatie aan de betrokkenen worden gegeven. Het gebruik van logo's moet worden gezien als een maatregel bovenop de verstrekking van uitvoeriger informatie.

([1]) Zie meer uitvoerig de punten 46-50 van dit advies.

De hoeksteen: Het opt-in beginsel

46. Alle RFID-toepassingen moeten beantwoorden aan en uitvoering geven aan een voorafgaande voorwaarde, namelijk een opt-in beginsel aan het verkooppunt. Wanneer wordt toegestaan dat RFID-tags na het verkooppunt doorgaan met het zenden van informatie, zou dit onwettig zijn tenzij de voor de verwerking verantwoordelijke daarvoor rechtsgronden heeft. Deze rechtsgronden zullen gewoonlijk alleen a) de toestemming van de betrokkene; of b) indien de gegevens nodig zijn voor een dienstverlening, een specifiek en vrijwillig verzoek van de persoon in kwestie zijn ([1]). Beide rechtsgronden gelden dan als keuze („opt-in").

47. Volgens het opt-in beginsel moeten tags aan het verkooppunt gedesactiveerd worden tenzij de koper van het product waaraan de tag bevestigd is, de tag actief wenst te laten. Wanneer de koper ermee instemt dat de tag actief blijft, stemt hij ermee in dat zijn gegevens verder worden verwerkt en dat de gegevens bijvoorbeeld worden doorgegeven aan de afleesapparatuur wanneer hij opnieuw een bezoek brengt aan de voor de verwerking verantwoordelijke.

48. De EDPS benadrukt dat een flexibele benadering belangrijk is om de toenemende verscheidenheid van RFID-toepassingen aan te kunnen en om de ontwikkeling van nieuwe, innovatieve bedrijfsmodellen mogelijk te maken. Het opt-in beginsel moet op flexibele wijze kunnen worden gehanteerd.

49. Voor het uitvoeren van het opt-in beginsel zijn er veel opties. Als alternatief voor het verwijderen van de tag kan worden overwogen de tag te blokkeren, tijdelijk buiten gebruik te stellen of volgens een methode die bekend staat als het „resurrecting duckling"-model ([2]), aan een specifieke gebruiker te binden. Van een tag met een korte levenscyclus kan het adres dat verwijst naar informatie in een gegevensbank ook worden gewist uit de referentiegegevensbank, waardoor wordt vermeden dat er nog meer door de tag verzamelde informatie wordt verwerkt.

50. Tot slot zijn er, hoewel de EDPS stelt dat het opt-in beginsel aan het verkooppunt een wettelijke verplichting is die voor de meeste gevallen reeds bestaat in de richtlijn gegevensbescherming, goede redenen om deze verplichting te specificeren in zelfreguleringsinstrumenten, ook om te waarborgen dat dit beginsel op de meest passende wijze wordt uitgevoerd. In ieder geval is een specifieke uitvoering nodig voor de RFID-toepassingen die niet onder de richtlijn gegevensbescherming vallen.

Noodzaak van „privacy-by-design"

51. In de Mededeling van de Commissie wordt in deel 3.2 (bladzijde 6) het idee onderschreven van het tijdig formuleren en goedkeuren van ontwerpcriteria. De EDPS juicht deze aanpak toe. Het goedkeuren van specificaties en ontwerpcriteria, ook wel beste beschikbare technieken genaamd (BBT), zal inderdaad bijdragen aan regulering van de gegevensbescherming en aan veiligheidsvereisten. Deze identificatie van technologische en organisatorische criteria zal, mits vaak bijgewerkt, het model dat de persoonlijke levenssfeer en beveiligingsvereisten met elkaar verenigt, waar de Europese Unie aan werkt, versterken.

52. Het vinden van de juiste BBT voor de persoonlijke levenssfeer en de beveiliging ten aanzien van RFID-systemen zal ook van doorslaggevende betekenis zijn voor het opbouwen van een vertrouwenwekkende omgeving die de aanvaarding ervan door de eindgebruikers zal vergroten, en voor het concurrentievermogen van het Europese bedrijfsleven.

53. Het selecteren van BBT voor RFID-systemen moet worden gestimuleerd door effectbeoordelingen op het gebied van persoonlijke levenssfeer en beveiliging, waarin nog veel moet worden geïnvesteerd. De EDPS vindt dat het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), tezamen met de gezamenlijke onderzoekscentra van de Europese Commissie die verbonden zijn met de belanghebbenden uit het bedrijfsleven, een bijdrage kunnen leveren aan het omschrijven van de beste praktijken en aan de ontwikkeling van dergelijke methodologieën. Met het onlangs gelanceerde programma „technische richtsnoeren voor RFID" heeft het Duitse overheidsbureau voor informatiebeveiliging (BSI) een goed voorbeeld gegeven ([3]) van BBT die nu op Europees niveau moeten worden uitgewerkt.

54. Normen kunnen ook een doorslaggevende rol spelen bij de tijdige aanneming van het beginsel van privacy-by-design. Daarom moet de Commissie ertoe bijdragen dat er bij de ontwikkeling van internationale RFID-normen waarborgen worden ingebouwd voor de persoonlijke levenssfeer en gegevensbescherming. De „Groep van artikel 29" heeft in haar werkdocument ([4]) over RFID duidelijk laten zien dat normen kunnen bijdragen aan de ontwikkeling van RFID-systemen die niet raken aan de persoonlijke levenssfeer.

([1]) In sommige RFID-toepassingen kunnen wellicht andere gronden gelden, zoals artikel 7, onder f) (gerechtvaardigd belang van de voor de verwerking verantwoordelijke, mits er goede waarborgen zijn).

([2]) De naam van dit model, dat is ontwikkeld door Frank Stajano en Ross Anderson van de Universiteit van Cambridge, is geïnspireerd door de gans die uit het ei komt en veronderstelt dat het eerste bewegende voorwerp de moedergans moet zijn.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Werkdocument (WP 105) over gegevensbeschermingsvraagstukken in verband met RFID-technologie van 19 januari 2005.

55. Voorts is de EDPS tevreden over het standpunt dat de Commissie heeft ingenomen inzake onderzoek naar en ontwikkeling van RFID-technologieën en de noodzaak om risico's voor de persoonlijke levenssfeer te ondervangen. Het beginsel van de privacy-by-design moet namelijk worden ingevoerd in de allereerste fase van de ontwikkeling van technologieën, zodat deze beter voldoen aan het rechtskader inzake gegevensbescherming. De EDPS zal, zoals kort in zijn jaarverslag over 2006 is gezegd, hieraan medewerking verlenen door per geval adviezen te verstrekken over projecten van het zevende kaderprogramma (2007-2013).

V. **ZIJN ER SPECIFIEKE WETGEVINGSMAATREGELEN NODIG?**

56. Zelfregulering is wellicht geen afdoend middel voor een volledige toepassing van het bestaande kader voor gegevensbescherming en de persoonlijke levenssfeer. Zelfs indien zelfregulering voldoet aan bovengenoemde vereisten, is het gebruik ervan vrijwillig en kan niet-naleving niet altijd doeltreffend worden bestraft. Bovendien zijn er misschien nog bindende wetgevingsmaatregelen nodig om ieders recht op persoonlijke levenssfeer en gegevensbescherming te waarborgen. Dit wordt des te noodzakelijker als de zelfgereguleerde aanpak mislukt.

57. Zeer belangrijk is de vaststelling welke juridische instrumenten noodzakelijk zijn om een doeltreffende invoering van RFID-toepassingen te waarborgen met de nodige technische oplossingen die de risico's voor gegevensbescherming en de persoonlijke levenssfeer moeten wegnemen of minimaliseren, en om ervoor te zorgen dat de voor de verwerking verantwoordelijken goede maatregelen treffen om hun uit de huidige rechtskaders voortvloeiende verplichtingen na te komen. Dit roept een aantal bijkomende vragen op:

— zijn er specifieke regels nodig?

— zo ja, kunnen deze regels worden aangenomen binnen het bestaande wetgevingskader, bijvoorbeeld via de bestaande comitologieprocedures?

— of moet er een nieuw wetgevingsinstrument komen om te waarborgen dat RFID-toepassingen worden gebruikt met ingebouwde technologieën die de persoonlijke levenssfeer beschermen?

58. Dit hoofdstuk gaat over de mogelijkheid om bindende wetgevingsmaatregelen uit te vaardigen binnen het bestaande rechtskader, en hoofdstuk VI gaat over de noodzaak van een nieuw wetgevingsinstrument, omdat dat een afzonderlijk onderwerp is.

59. Allereerst moet er aandacht worden geschonken aan de bepalingen van artikel 17 van Richtlijn 95/46/EG, artikel 14, lid 3 van Richtlijn 2002/58/EG en artikel 3, lid 3, onder c), van Richtlijn 1999/5/EG. Volgens artikel 14, lid 3 kunnen de lidstaten maatregelen nemen om ervoor te zorgen dat de eindapparatuur gebouwd is op een wijze die verenigbaar is met het recht van gebruikers om het gebruik van hun persoonsgegevens te beschermen en te controleren, in overeenstemming met Richtlijn 1999/5/EG ([1]). In artikel 3, lid 3, onder c), van Richtlijn 1999/5/EG staat dat de Commissie (middels de comitologieprocedure) kan besluiten dat apparatuur van bepaalde apparatuurcategorieën of apparatuur van een bepaalde soort zo geconstrueerd moet zijn dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen. Artikel 3, lid 3, onder c), van Richtlijn 1999/5/EG is tot nog toe niet gebruikt.

60. Deze bepalingen geven de wetgever (op nationaal en op communautair niveau) de bevoegdheid om voor te schrijven dat er waarborgen voor de persoonlijke levenssfeer en gegevensbescherming worden ingebouwd in de vervaardiging van RFID-systemen, een concept dat bekend staat als privacy-by-design ([2]). Dat vergt ook het gebruik van de beste beschikbare technieken.

61. De EDPS raadt de Commissie aan om, teneinde toepassing van het concept privacy-by-design verplicht te maken, gebruik te maken van het mechanisme van artikel 3, lid 3, onder c) van Richtlijn 1999/5/EG, in overleg met de RFID-deskundigengroep.

62. Ten tweede kan de toepassing van het bestaande wetgevingskader worden toegespitst op RFID, en wel middels wijzigingen van de richtlijnen zelf. Zoals gezegd heeft de Commissie onlangs een voorstel ingediend tot wijziging van de e-privacy-richtlijn via een nieuwe bepaling vanuit dit oogpunt. De EDPS begroet met instemming deze eerste bevestiging van de toepasselijkheid van de richtlijn op RFID-toepassingen. De EDPS zal in zijn advies over het voorstel tot wijziging, dat begin 2008 zal verschijnen, de specifieke vraagstukken over het verband tussen de e-privacy-richtlijn en RFID, behandelen.

63. Gelet op het feit dat de Commissie in de nabije toekomst geen wijzigingen van de richtlijn gegevensbescherming voorziet ([3]), zijn de mogelijkheden om de toepassing van het bestaande wetgevingskader op RFID toe te spitsen, beperkt.

VI. **IS ER EEN SPECIFIEK RECHTSKADER VOOR RFID NODIG?**

Voornemens van de Commissie

64. In de Mededeling ([4]) wordt het belang benadrukt van beveiliging en privacy-by-design. Ook wordt gevraagd om betrokkenheid van alle belanghebbenden. Het belangrijkste resultaat van de activiteiten van de Commissie zal een aanbeveling zijn waarin de beginselen worden geformuleerd

([1]) En met Beschikking 87/95/EEG van de Raad van 22 december 1986 betreffende de normalisatie op het gebied van de informatietechnologieën en de telecommunicatie (PB L 36 van 7.2.1987, blz. 31).
([2]) Zie hoofdstuk IV.
([3]) De EDPS steunt deze aanpak, zie punt 64
([4]) Zie punt 4.1 van de Mededeling.

die overheidsdiensten en andere belanghebbenden moeten toepassen ten aanzien van het gebruik van RFID. De Aanbeveling wordt waarschijnlijk in de voorjaar van 2008 aangenomen. De wetgevingsambities in de Mededeling bestaan uit twee stappen. De Commissie zal:

— passende bepalingen over RFID overwegen in het komende voorstel voor wijziging van de e-privacy-richtlijn. Zoals reeds is gezegd, heeft de Commissie in november een wijziging van de e-privacy-richtlijn voorgesteld, waarin wordt bevestigd dat de richtlijn geldt voor RFID-toepassingen ([1]), maar waarin niet wordt voorgesteld de reikwijdte van de e-privacy-richtlijn uit te breiden naar particuliere netwerken;

— bezien of er verdere wetgevingsstappen moeten worden genomen om de gegevensbescherming en de persoonlijke levenssfeer te waarborgen.

65. Met deze aanpak kan worden verwacht dat de Commissie niet, of in elk geval niet op de korte termijn, voornemens is op RFID-gebied nieuwe specifieke wetgeving voor te stellen ter waarborging van de gegevensbescherming en de persoonlijke levenssfeer.

Parameters voor de wetgever

66. In zijn Advies inzake de mededeling over de richtlijn gegevensbescherming heeft de EDPS een aantal richtsnoeren gegeven over wetgevingsactiviteiten in verband met de verwerking van persoonsgegevens, die als volgt kunnen worden samengevat:

— ten eerste moeten de kernbeginselen van gegevensbescherming behouden blijven: „Er zijn geen nieuwe principes nodig, maar er bestaat duidelijk behoefte aan een nieuwe administratieve regeling die enerzijds doeltreffend is en passend voor een netwerkmaatschappij, en anderzijds de administratieve kosten zo beperkt mogelijk houdt." ([2]);

— ten tweede moeten wetgevingsvoorstellen alleen worden ingediend indien de noodzaak en de evenredigheid ervan genoegzaam zijn aangetoond. Daarom moet het algemene wetgevingskader voor gegevensbescherming op de korte termijn niet worden veranderd;

— ten derde kunnen veranderingen in de samenleving leiden tot specifieke rechtskaders, ter aanpassing van de beginselen van de richtlijn gegevensbescherming aan vraagstukken die worden opgeroepen door specifieke technologieën zoals RFID. Ook is het in dit verband duidelijk dat moet worden voldaan aan de voorwaarden van noodzaak en evenredigheid.

67. Als volgende stap is het nuttig te specificeren met welke verwachtingen de wetgever te maken krijgt op RFID-gebied:

— wetgeving moet flexibel zijn en ruimte bieden voor innovaties en technologische ontwikkeling. Dit moet leiden tot wetgeving die in voldoende mate technologieneutraal is;

— ten tweede moet wetgeving rechtszekerheid bieden. Dit moet leiden tot wetgeving die voldoende specifiek is. De belanghebbenden moeten precies weten hoe hun gedrag wordt gereguleerd;

— ten derde moet wetgeving alle gerechtvaardigde belangen die op het spel staan, goed beschermen. Daarvoor moet de naleving van de wetgeving in ieder geval worden afgedwongen en moeten de verantwoordelijkheden duidelijk worden omschreven: welke partij is aansprakelijk voor welk gedrag? ([3]) Deze vereisten zijn nog belangrijker wanneer de persoonlijke levenssfeer en gegevensbescherming, zijnde fundamentele rechten die iedereen heeft krachtens het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en het Handvest van de grondrechten van de Europese Unie, in het geding zijn.

Standpunt van de EDPS

68. Voor de EDPS is het duidelijk dat niet alle technologische ontwikkelingen reacties van de zijde van de Europese wetgever moeten oproepen. Technologische ontwikkelingen kunnen snel gaan maar de aanneming en inwerkingtreding van wetgeving vergt tijd, en zo hoort het ook. Wetgeving moet het resultaat zijn van een afweging van alle belangen die op het spel staan. Wanneer wordt gekozen voor het instrument van de richtlijn, is er nog meer tijd nodig, aangezien richtlijnen volledig in de rechtsstelsels van de lidstaten moeten worden geïmplementeerd.

69. RFID is echter niet zomaar weer een nieuwe technologische ontwikkeling, en dat is op diverse plaatsen in dit advies benadrukt. In de Mededeling wordt RFID bestempeld als de poort naar een nieuwe ontwikkelingsfase van de informatiemaatschappij, ook wel het „internet van dingen" genaamd, en RFID-tags worden belangrijke elementen van de intelligente omgevingen („ambient intelligence"). Deze omgevingen zijn ook belangrijke stappen in de ontwikkeling van wat vaak de gecontroleerde samenleving wordt genoemd ([4]). Tegen deze achtergrond kan het gerechtvaardigd zijn op RFID-gebied wetgeving te maken. RFID kan een kwalitatieve verandering teweegbrengen.

([1]) Zie het voorgestelde nieuwe artikel 3 van Richtlijn 2002/58/EG.
([2]) Punt 24 van het Advies inzake de mededeling over de richtlijn gegevensbescherming.
([3]) In gegevensbeschermingstaal betekent dit dat moet worden aangegeven wie „de voor verwerking verantwoordelijke" is.
([4]) Dit is herhaald in een verklaring die de Europese gegevensbeschermingsautoriteiten op 2 november 2006 in Londen hebben aangenomen en die op de website van de EDPS staat: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. In dit verband raadt de EDPS aan te overwegen (een voorstel voor) communautaire wetgeving aan te nemen ter regulering van de belangrijkste vraagstukken van RFID-gebruik in de sectoren in kwestie, mocht de correcte uitvoering van het bestaande rechtskader niet lukken. Eenmaal in werking moet zo'n wetgevingsmaatregel worden gezien als een *lex specialis* ten aanzien van het algemene kader voor gegevensbescherming.

71. Als er zo'n wetgevingsinstrument wordt aangenomen, zou dat de volgende voordelen hebben:

— het instrument kan de inhoudelijke parameters geven voor de zelfregulerende mechanismes;

— het vooruitzicht dat er een wetgevingsinstrument zal worden aangenomen, zou voor de belanghebbenden een goede stimulans kunnen zijn om zelfregulerende mechanismes op te zetten die goede bescherming bieden.

72. Om alles wat gemakkelijker te maken, kan de Commissie worden gevraagd een raadplegingsdocument over de voor- en nadelen van specifieke wetgeving en van de belangrijkste onderdelen van zo'n wetgeving, op te stellen. Uiteraard kan de belanghebbenden worden verzocht bij te dragen aan deze raadpleging. Zo kan ook „de Groep van artikel 29" bij een en ander worden betrokken.

Mogelijke werkwijzen

73. Dit ingrijpen van de wetgever kan een op maat gemaakt rechtskader opleveren, bestaande uit een mengeling van regulerende instrumenten die het bestaande rechtskader specificeren en vervolledigen. Zo'n op maat gemaakt rechtskader moet steunen op de bekende gegevensbeschermingsbeginselen en toegesneden zijn op de verdeling van verantwoordelijkheden en op de doeltreffendheid van de controlemechanismes.

74. Dat zulke op maat gemaakte wetgeving nodig zou kunnen zijn, ligt aan het feit dat niet alle RFID-toepassingen de verwerking van persoonsgegevens met zich meebrengen. Met andere woorden, indien RFID-toepassingen geen verwerking van persoonsgegevens met zich meebrengen, zijn de partijen die producten maken en verkopen waarin RFID-tags zitten, niet wettelijk verplicht technologische maatregelen te nemen om te voorkomen dat er wordt „afgeluisterd" of dat er afleesapparatuur wordt geplaatst zonder voorafgaande waarschuwing aan het publiek. Zoals is aangetoond, bestaan er evenwel ook met zulke RFID-toepassingen risico's voor de persoonlijke levenssfeer die voortvloeien uit de mogelijke observatie van personen, en dus moeten er gelijkaardige waarborgen voor de persoonlijke levenssfeer komen. Dat kan het geval zijn als er een tag per product wordt geplaatst in consumentenproducten voor het verkooppunt. Kortom, ook RFID-toepassingen die geen persoonsgegevens verwerken, kunnen iemands persoonlijke levenssfeer bedreigen door heimelijke observatie en het gebruik van informatie voor onaanvaardbare doeleinden mogelijk te maken.

75. De EDPS vindt dat dit ongewenste resultaat moet worden vermeden. Aangezien de huidige wetgeving gedeeltelijk (ten minste wat betreft RFID-toepassingen die geen verwerking van persoonsgegevens met zich meebrengen) nalaat deze bedreiging van de persoonlijke levenssfeer te bestrijden, en oplossingen in de vorm van niet-bindende afspraken niet voldoende zijn, lijkt het nodig dwingende wetgevingsmaatregelen op te leggen om een bevredigend resultaat te bereiken.

76. Zulke maatregelen moeten in elk geval:

— het opt-in beginsel aan het verkooppunt omvatten als een welomschreven en onmiskenbare wettelijke verplichting, ook voor RFID-toepassingen die buiten de richtlijn gegevensbescherming vallen ([1]);

— verplichten dat RFID-toepassingen worden gebruikt met de nodige technische voorzieningen of privacy-by-design.

VII. **GOED BEHEER**

77. Waar de Mededeling RFID-systemen alleen binnen de interne markt als „van nature grensoverschrijdend" ziet, vindt de EDPS dat deze dimensie op een internationaler niveau moet worden aangepakt. In een winkel zijn RFID-systemen reeds „grensoverschrijdend" aangezien de activiteit van de tag wellicht niet ophoudt aan het verkooppunt. De RFID-technologieën in het algemeen worden ook „grensoverschrijdend" wanneer er overdracht zou kunnen plaatsvinden van persoonsgegevens naar een derde land omdat de producent van het product met een tag, dat onderdeel is van het RFID-systeem, buiten de Europese Unie gevestigd is ([2]).

78. Vanuit een meer op de toekomst gericht standpunt is het goede beheer van databanken voor de referentie-identiteit van RFID ook een kritieke dimensie voor een correcte handhaving van het Europese rechtskader voor gegevensbescherming. De EDPS dringt aan op het vinden van een oplossing aangezien niet kan worden aanvaard dat dit kader verder wordt aangetast.

79. De EDPS ziet het beheer van RFID als een grote uitdaging die aanzienlijke investeringen zal vergen. Het juiste onderhandelingsforum en de meest geschikte beheersinfrastructuur moeten worden gevonden zodat de rechten op gegevensbescherming in deze internationale omgevingen afdoende worden geëerbiedigd.

([1]) In hoofdstuk IV is gesteld dat het opt-in beginsel aan het verkooppunt een wettelijke verplichting is die reeds bestaat uit hoofde van de richtlijn gegevensbescherming.

([2]) De verplichtingen waarmee de overdracht van persoonsgegevens is omgeven, staan in de artikelen 25 en 26 van de richtlijn gegevensbescherming.

80. In dit verband verzoekt de EDPS de Commissie om haar ideeën over het beheer, mogelijkerwijs in overleg met de Groep RFID-deskundigen, te presenteren.

VIII. **CONCLUSIE**

81. De EDPS is blij met de Mededeling van de Commissie over RFID omdat in die mededeling de belangrijkste vraagstukken worden behandeld die zich voordoen in de context van het gebruik van de RFID-technologie, zonder dat wordt voorbijgegaan aan de doorslaggevende vraagstukken inzake persoonlijke levenssfeer en gegevensbescherming. De EDPS is het eens met het standpunt dat RFID-systemen een belangrijke rol zouden kunnen spelen in de ontwikkeling van de informatiemaatschappij, ook wel het „internet van dingen" genaamd.

De gevolgen duidelijk maken

82. Het wijdverbreide gebruik van RFID-technologie is fundamenteel nieuw en kan een fundamentele invloed hebben op onze samenleving en op de bescherming van grondrechten in onze samenleving, zoals de persoonlijke levenssfeer en gegevensbescherming. RFID kan een kwalitatieve verandering teweegbrengen.

83. Er kunnen vijf basispunten van privacy en beveiliging worden onderscheiden:

— de identificatie van de betrokkene;

— de identificatie van de voor de verwerking verantwoordelijke(n);

— het afgenomen belang van het traditionele onderscheid tussen de persoonlijke en de openbare levenssfeer;

— de gevolgen van de afmeting en de fysieke eigenschappen van RFID-tags;

— het gebrek aan transparantie van de verwerking.

De gevolgen specificeren

84. Het algemene wetgevingskader voor gegevensbescherming, zoals neergelegd in Richtlijn 95/46/EG, geldt voor RFID voor zover door RFID-systemen verwerkte gegevens vallen onder de definitie van persoonsgegevens.

85. Wat betreft de e-privacy-richtlijn: in het voorstel van de Commissie van 13 november 2007 tot wijziging van de richtlijn staat een bepaling waarmee wordt beoogd te specificeren dat de richtlijn daadwerkelijk geldt voor bepaalde RFID-toepassingen. Andere bepaalde RFID-toepassingen vallen wellicht niet onder de richtlijn omdat de richtlijn beperkt is tot de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten van openbare communicatienetwerken.

86. De bescherming van persoonsgegevens kan worden aangevuld met een reeks zelfreguleringsinstrumenten. Er dient ruimte te worden geboden voor zelfregulering, mits:

— er concrete en praktische adviezen worden gegeven over specifieke RFID-toepassingen;

— er een oplossing wordt geboden voor de specifieke gegevensbeschermingsvraagstukken en -problemen die zich voordoen in de context van algemene RFID-toepassingen;

— er wordt bijgedragen aan de eenvormige en geharmoniseerde toepassing van de richtlijn gegevensbescherming in de gehele EU;

— deze door alle belanghebbenden wordt toegepast.

87. De EDPS beveelt de Commissie aan om, in nauwe samenwerking met de RFID-deskundigengroep, een of meer documenten op te stellen met duidelijke sturing over hoe het huidige rechtskader moet worden toegepast op de RFID-omgeving.

88. De richtsnoeren met beginselen die gelden voor het gebruik van RFID moeten voldoende doelgericht zijn en een sectorspecifieke aanpak volgen. Er moeten praktische en doeltreffende methodes worden voorgesteld voor het ontwikkelen van *technieken en normen* die ertoe kunnen bijdragen dat de RFID-systemen stroken met het rechtskader voor gegevensbescherming en die zullen leiden tot het gebruik van privacy-by-design.

89. De EDPS is ingenomen met de aanpak in de Mededeling van de Commissie, inhoudende dat het idee wordt onderschreven van het tijdig formuleren en goedkeuren van ontwerpcriteria.

90. Hoewel de EDPS van mening is dat het opt-in beginsel aan het verkooppunt een wettelijke verplichting is die in de meeste situaties reeds bestaat uit hoofde van de richtlijn gegevensbescherming, moet deze verplichting in zelfreguleringsinstrumenten worden gespecificeerd.

Zijn er specifieke maatregelen nodig?

91. De EDPS raadt de Commissie aan om, teneinde het gebruik van het concept privacy-by-design verplicht te stellen, gebruik te maken van het mechanisme van artikel 3, lid 3, onder c), van Richtlijn 1999/5/EG, in overleg met de RFID-deskundigengroep.

92. De EDPS raadt aan te overwegen (een voorstel voor) communautaire wetgeving aan te nemen ter regulering van de belangrijkste vraagstukken van RFID-gebruik in de sectoren in kwestie, mocht de correcte uitvoering van het bestaande rechtskader niet lukken. Eenmaal in werking moet zo'n wetgevingsmaatregel worden gezien als een lex specialis ten aanzien van het algemene kader voor gegevensbescherming. Deze wetgevingsmaatregel moet ook de bezorgdheid over gegevensbescherming en de persoonlijke levenssfeer wegnemen n.a.v. bepaalde RFID-toepassingen, zoals het plaatsen van een tag per product voor het verkooppunt, wat niet noodzakelijkerwijs inhoudt dat er persoonsgegevens worden verwerkt.

93. De Commissie moet een raadplegingsdocument opstellen over de voor- en nadelen van specifieke wetgeving en van de belangrijkste onderdelen van zulke wetgeving.

94. Dit ingrijpen van de wetgever kan een op maat gemaakt rechtskader opleveren, bestaande uit een mengeling van regulerende instrumenten die het bestaande rechtskader specificeren en vervolledigen. De maatregelen moeten in elk geval:

— het opt-in beginsel aan het verkooppunt omvatten als een welomschreven en onmiskenbare wettelijke verplichting, ook voor RFID-toepassingen die buiten de richtlijn gegevensbescherming vallen ([1]);

— verplichten dat RFID-toepassingen worden gebruikt met de nodige technische voorzieningen of privacy-by-design.

Goed beheer

95. De EDPS verzoekt de Commissie om haar ideeën over het beheer te presenteren, mogelijkerwijs in overleg met de Groep RFID-deskundigen.

Brussel, 20 december 2007.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming

([1]) In hoofdstuk IV is gesteld dat het opt-in beginsel aan het verkooppunt een wettelijke verplichting is die reeds bestaat uit hoofde van de richtlijn gegevensbescherming.