Advies nr 27/2009 van 14 oktober 2009

Betreft: Advies uit eigen beweging inzake RFID (A/2009/003)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op de Aanbeveling van de Europese Commissie d.d. 12 mei 2009 inzake RFID;

Gelet op het verslag van de heer Frank ROBBEN;

Brengt op 14 oktober het volgend advies uit eigen beweging uit:

I. TOEPASSINGSGEBIED VAN HET ADVIES

1. Dit advies uit eigen beweging handelt over het gebruik van RFID toepassingen met het oog op de verwerking van persoonsgegevens.

2. De Commissie brengt dit advies uit, rekening houdend met de huidige kennis van de RFID technologie. Zij behoudt zich natuurlijk de mogelijkheid voor haar houding ter zake in de toekomst aan te passen in functie van de evolutie van de technologie en haar ervaringen op dit gebied. Het huidige advies bestaat uit een globale analyse van de RFID toepassingen, en verhindert uiteraard niet dat de Commissie zich zou uitspreken over specifieke dossiers.

II. RFID: ALGEMENE VERKLARINGEN

A. Definitie en belang van de RFID

3. **Radio frequency identification**, *identificatie door middel van radiogolven* (afgekort **RFID**), is een technologie om van op een afstand informatie op te slaan en te lezen van zogenaamde RFID-"tags" die op of in objecten of levende wezens zitten. De visie achter deze technische vooruitgang is om elk voorwerp op de wereld afzonderlijk te kunnen identificeren. Het optimaliseren van de 'supply chain' met behulp van een globale visibiliteit is de belangrijkste groeifactor voor deze technologie. Het ideale scenario daarbij is dat de juiste materialen zich in de juiste staat, op de juiste plaats, op het juiste moment bevinden. Een RFID-systeem bestaat uit *drie basisonderdelen* : een 'reader' of lezer, een RFID tag (hierna tag) en een systeem om het dataverkeer in te verwerken. Via de lezer wordt informatie afgelezen van de chip in de tag. In de meeste gevallen zal deze informatie beperkt zijn tot een identificatienummer maar afhankelijk van de geheugencapaciteit kan er ook aanvullende informatie op een chip worden opgeslagen. RFID technologie kan op diverse manieren worden gebruikt, naargelang de types van tags en readers (cfr. infra).

4. RFID wordt reeds in vele sectoren voor diverse doeleinden aangewend. De technologie is nog relatief jong en in volle ontwikkeling, maar de toepassingsmogelijkheden zijn divers en veelbelovend. Hiernavolgend worden enkele voorbeelden opgesomd :

- *Transport* : Veel toepassingen bij het openbaar vervoer werken reeds met RFID technologie, bijvoorbeeld het MOBIB systeem te Brussel. Daarnaast zijn autosleutels vaak uitgerust met een dergelijk systeem (transponder).
- *Luchtvaart* : De technologie kan worden gebruikt voor het verwerken van de bagage binnen een luchthaven. 'Boarding passes' kunnen eveneens worden utgerust met een tag om zo de locatie van passagiers te kunnen bepalen.

- *Gezondheidszorg* : RFID systemen worden onder meer gebruikt voor de opsporing van medicijnen en om vervalsing tegen te gaan. Hiertoe worden de producten door de fabrikant voorzien van een tag, welke kan gelezen worden door de apotheker, uitgerust met een lezer. Deze lezers zullen vaststellen dat het product wel degelijk afkomstig is van de bewuste fabrikant. Een meer tot de verbeelding sprekende toepassing betreft de zogenaamde 'verichip[1]', een bij mensen implanteerbare RFID chip, ter grootte van ongeveer 2 korrels rijst. Deze chip, in 2004 goedgekeurd door de Amerikaanse FDA[2], kan bijvoorbeeld de medische gegevens van een patiënt bevatten, waardoor hij nuttig kan zijn in noodsituaties. In Nederland wordt een dergelijke chip gebruikt door een nachtclub, waardoor de bezoekers – die dergelijke chip hebben laten aanbrengen- automatisch worden herkend. Door die herkenning krijgen zij bijvoorbeeld toegang tot bepaalde ruimtes en kunnen zij hun consumpties afrekenen.
- *Beveiliging -Toegangscontrole* : Bankbiljetten kunnen met tags worden uitgerust om vervalsing tegen te gaan. RFID wordt reeds gebruikt in paspoorten, waaronder de Belgische internationale reispas. Daarnaast kan de toegang van personen tot bepaalde ruimtes eveneens worden geregeld met gebruik van RFID technologie, bijvoorbeeld door hen uit te rusten met een zogenaamde 'smart card'.
- *Distributiesector/productiesector* : Hier wordt de technologie onder meer toegepast in stockbeheer, binnen het logistieke systeem kunnen producten worden gevolgd. Hierdoor kan het logistieke systeem sneller functioneren. Daarnaast kunnen producten sneller afgerekend worden en zijn de producten beter tegen diefstal beveiligd. Ook het inventariseren van producten kan sneller (men hoeft slechts met een RFID-reader langs de schappen te lopen). En de data van onder andere het aankoopgedrag kan in combinatie met een klantenkaart voor marketing doeleinden gebruikt worden. Ook kan er makkelijker gecontroleerd worden op bijvoorbeeld de versheid en herkomst van het product. Tenslotte bestaat de mogelijkheid om via een RFID-chip op een GSM contactloos te betalen in winkels etc.. In Japan is dit systeem dermate ingeburgerd dat mensen hun GSM gebruiken om bijvoorbeeld een treinkaartje aan te kopen. In België loopt een proefproject hieromtrent (contactloos GSM betalen[3]).

[1] Zie http://www.verichipcorp.com/our_businesses.html

[2] Zie advies groep 29 verwijzing

[3] http://www.pingping.be/docs/How_it_works.pdf

B. Werkwijze

5. De tags kunnen "passief", "actief", of "conditieregistrerend" zijn. *Passieve* RFID-tags hebben geen eigen energiebron en zenden een antwoord door het omzetten van de energie van de radiogolven welke door de lezer uitgezonden worden. *Actieve* RFID-tags voeden zich met een batterij en kunnen worden gelezen en beschreven met een lezer, actieve tags zenden meestal met een interval hun ID uit. *Conditieregistrerende* tags[4] hebben niet alleen een batterij, maar ook circuits die diagnostische gegevens uitlezen en deze verzenden naar het sensorsysteem. De tags bewaken de omgevingsomstandigheden, communiceren met andere objecten en verzamelen de gegevens die niet door een enkele sensor gedetecteerd kunnen worden. De informatie wordt vervolgens met behulp van netwerksoftware teruggestuurd naar het back-end systeem.

6. RFID-tags onderscheiden zich onderling ook door de gebruikte frequentie. In het algemeen kan gezegd worden: hoe hoger de frequentie, des te verder het leesbereik.

7. Het is gebruikelijk dat tags voorzien zijn van een meestal onuitwisbaar *identificatienummer*. Binnen een enkel RFID systeem zijn dit bijna altijd unieke (volg)nummers. Deze nummers kunnen bij ingebruikname van de tags worden bepaald door het nummer naar de tag te schrijven met een reader of printer. Het is ook mogelijk dit aan de producent van de tags over te laten.

8. Voordelen van het toepassen van RFID zijn onder meer:

- Unieke code zodat ieder individueel object altijd en overal gevolgd kan worden
- Er is geen fysiek contact nodig (zoals bij bankpasjes)
- Er is geen zichtlijn nodig (zoals bij de streepjescode)
- Vele (honderden) codes kunnen in een of enkele seconden worden gelezen
- Veel grotere afstanden zijn mogelijk dan bij de streepjescode
- Vervalsen van RFID-tags is veel complexer dan de streepjescode.

9. Mogelijke nadelen :

- Als het identificatienummer van een RFID-tag geassocieerd kan worden met een persoon, kan dit individu gevolgd worden
- Lees/schrijf mogelijkheden van de RFID-tag kunnen het mogelijk maken dat er ongemerkt fraude wordt gepleegd, ook ten aanzien van personen

[4] Zie http://www-05.ibm.com/be/ideasfromibm/rfid/nl/index.html

- Door het grote (zend/ontvang)bereik kan er verwarring optreden. Er worden niet bedoelde RFID-tags gelezen die de gegevensverwerking kunnen verstoren.

C. MOGELIJKE PRIVACY IMPLICATIES[5]

10. Verschillende RFID toepassingen, zoals hierboven besproken, zullen nooit een verwerking van persoonsgegevens impliceren. Er zijn evenwel toepassingen waarbij dit wel het geval zal of kan zijn. Hiernavolgend worden twee situaties onderscheiden waarbij sprake kan zijn van een verwerking van persoonsgegevens.

C.1. LINKEN VAN PERSOONSGEGEVENS MET TAG

11. Het identificatienummer van de tag kan worden verbonden met persoonsgegevens/een persoon, bijvoorbeeld het identificatienummer van een bepaald product wordt verbonden met de klant die het product heeft aangekocht. Een winkel kan de identificatienummers van de producten verbinden met betaalkaartgegevens, en de klantendatabank. Dit zou bijvoorbeeld dienstig kunnen zijn voor garantie doeleinden. Een andere toepassing zou het gebruik van RFID in een klantenkaart kunnen zijn, waardoor de klant in de winkel kan worden gevolgd, en nuttige marketinggegevens kunnen worden bekomen, zoals de in een bepaalde sectie doorgebrachte tijd, aantal bezoeken zonder aankoop, … .

C.2. PLAATSEN VAN PERSOONSGEGEVENS OP EEN TAG

12. Zoals hierboven aangegeven, wordt RFID reeds in de transportsector aangewend. In bepaalde luchthavens zijn proefprojecten hangende inzake het 'taggen' van 'boarding passes', waardoor de locatie van passagiers op de luchthaven kan worden achterhaald. In België werkt de Mobib kaart met RFID. Op de kaartchip zijn persoonsgegevens opgenomen.

III. TOEPASBAARHEID VAN DE WET BETREFFENDE DE VERWERKING VAN PERSOONSGEGEVENS (WVP)

A. De RFID toepassing maakt gebruik van persoonsgegevens

13. Overeenkomstig artikel 1 §1 van de WVP moet "onder persoonsgegevens" iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon worden verstaan, (…) als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer

[5] Zie hieromtrent tevens Article 29 data protection working party, Working document on data protection issues related to RFID technology, 19 januari 2005;

specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

14. De tag kan persoonsgegevens (naam, adres, …) opslaan. Daarnaast kan het identificatienummer van een tag aan een bepaalde persoon worden gekoppeld. De tag op zich kan dus informatie onthullen over een natuurlijke persoon maar ook de omstandigheden van de inzameling kunnen bijkomende persoonlijke informatie opleveren (zo kan de verwerking van gegevens betreffende de plaats en het ogenblik van de inzameling toelaten de aanwezigheid van een persoon op een bepaald ogenblik op een bepaalde plaats te achterhalen).

15. Vanaf het ogenblik dat het verband tussen het identificatienummer van de tag en een fysieke persoon met behulp van redelijke middelen kan worden gelegd door de verantwoordelijke voor de verwerking of enig ander persoon, gaat het om een persoonsgegeven. Indien er persoonsgegevens op een tag staan vermeld, is er uiteraard sprake van een verwerking van persoonsgegevens.

16. In voormelde gevallen beschouwt de Commissie de RFID toepassing in principe als een verwerking van persoonsgegevens.

B. De RFID toepassing kan een verwerking van gevoelige gegevens[6] uitmaken

17. Een bepaalde RFID toepassing (zie bijvoorbeeld supra, de verichip) kan informatie vrijgeven over de gezondheidstoestand van een persoon.

18. Wanneer de RFID toepassing gebruikt wordt om er informatie uit af te leiden die betrekking heeft op bijvoorbeeld de gezondheidstoestand, dienen die gegevens beschouwd te worden als gevoelige gegevens.

C. Het gebruik van de RFID impliceert een gegevensverwerking

19. De WVP definieert de "verwerking" als elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei

[6] In het raam van de bescherming van het privéleven zijn gevoelige gegevens de gegevens die bedoeld worden in de artikelen 6,7 en 8 van de WVP.

andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.[7]

20. Het gebruik van een RFID systeem veronderstelt de inzameling, de registratie en de opslag van gegevens (al dan niet persoonsgegevens) en dit met behulp van geautomatiseerde middelen.

IV. TOEPASSING VAN DE BEGINSELEN VAN DE WET BETREFFENDE DE VERWERKING VAN PERSOONSGEGEVENS (WVP)

A. Rechtmatigheid en proportionaliteit[8]

21. Elk persoonsgegeven moet verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

22. Om gerechtvaardigd te zijn moet elk doeleinde onder meer voldoen aan een van de voorwaarden van artikel 5 van de WVP.

23. Een verwerking van persoonsgegevens via een RFID toepassing is in principe mogelijk wanneer de betrokkenen hun *toestemming*[9] hebben verleend. Deze toestemming draagt ongetwijfeld bij tot de sociale aanvaarding van deze nieuwe technologie door de gebruikers. Overigens zal de verwerking eveneens kunnen toegestaan worden indien zij *voorzien* is *door een wet*[10] of wanneer de verantwoordelijke voor de verwerking een *gerechtvaardigd belang* kan doen gelden dat zwaarder doorweegt dan de belangen of de fundamentele rechten en vrijheden van de betrokkene[11], waarbij er onder meer dient over gewaakt dat de menselijke waardigheid van het individu niet in het gedrang komt.

24. De Commissie onderstreept dat een *geldige toestemming* een vrije, specifieke en op informatie berustende toestemming[12] is. Een vrije toestemming houdt onder andere in dat een alternatief systeem wordt aangeboden aan de betrokkenen, dat gelijkwaardig moet zijn en geen sanctie

---

[7] Artikel 1 §2 van de WVP.

[8] Artikelen 4 en 5 van de WVP.

[9] Artikel 5 a) van de WVP.

[10] Artikel 5 c) van de WVP.

[11] Artikel 5 f) van de WVP.

[12] Zie de definitie van toestemming in artikel 1 §8 van de WVP.

voor de betrokkene mag inhouden. In de distributiesector[13] bijvoorbeeld zou de klant zijn expliciete toestemming moeten geven (opt-in) aan de winkelier om een tag op een product operationeel te houden na de aankoop. Indien gewenst, moet de winkelier tot deactivatie of verwijdering van de tag overgaan, en dit zonder kosten voor de consument. De consument zou moeten kunnen verifiëren of deze deactivatie of verwijdering effectief is gebeurd.

25. De aandacht dient er eveneens op gevestigd te worden dat het verkrijgen van een *toestemming* een overmatige verwerking niet rechtvaardigt. De verantwoordelijke voor de verwerking dient te waken over de proportionaliteit van de geplande verwerking : het algemeen belang of het gerechtvaardigd belang van de verantwoordelijke voor de verwerking moeten afgewogen worden tegenover het recht op de bescherming van het privéleven van de betrokkenen. Een risicoanalyse is dan ook aanbevelenswaardig alvorens over te gaan tot de aanschaf van een dergelijk systeem, waarbij onder meer het beoogde RFID-systeem dient te worden vergeleken met de andere bestaande gegevensverwerkingssystemen op de markt.

26. Bij het inroepen van een *gerechtvaardigd belang* dient tenslotte te worden opgemerkt dat het doel waarmee de persoonsgegevens door bijvoorbeeld een winkelier worden verwerkt, in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze kan worden verwezenlijkt. Indien een winkelier bijvoorbeeld een klantenkaart met RFID aanbiedt, zou de klant de keuze moeten hebben tussen een anonieme kaart (zonder persoonsgegevens erin verwerkt, en welke niet wordt gekoppeld aan een bepaalde persoon door middel van databestand of betalingsinformatie) en een klantenkaart met persoonsgegevens.

B. Informatieverstrekking aan de betrokkenen

27. Bij elke gegevensverwerking moeten de personen ingelicht worden over de doeleinden van de verwerking, over de identiteit van de verantwoordelijke voor de verwerking en de bestemmelingen (of categorieën bestemmelingen) van de gegevens alsook over het bestaan van een recht op toegang en verbetering[14]. In het geval van RFID is deze informatieverplichting uitermate belangrijk, gezien de mogelijkheid om 'onzichtbaar' gegevens te verwerken via tags.

28. Er dient voor elke RFID applicatie een verstaanbare privacy policy te worden aangeboden, welke minimaal de volgende elementen zou moeten bevatten[15] :

---

[13] Zie de Aanbeveling van de Europese Commissie d.d. 12 mei 2009 on the implementation of privacy and data protection principles in applications supported by radio frequency identification, punten 9-14;

[14] Artikel 9 van de WVP

[15] Zie de aanbeveling van de Europese Commissie d.d. 12 mei 2009, o.c., punten 7-8;

- Identiteit en adres van de verantwoordelijke voor de verwerking;
- Doel van de verwerking;
- Welke gegevens worden verwerkt, in het bijzonder of er persoonsgegevens worden verwerkt, en of de locatie van de tags zal worden opgevolgd;
- Een samenvatting van de 'assessment' inzake de impact op de privacy en de bescherming van persoonsgegevens (cfr. infra, punt 32);
- De mogelijke privacy risico's, met betrekking tot het gebruik van tags in de toepassing, en de maatregelen welke de betrokkenen kunnen nemen om deze risico's te beperken;

29. Een ander element van de informatieplicht betreft de aangifte. Ingeval van een geautomatiseerde verwerking van persoonsgegevens moet er in principe een voorafgaandelijke aangifte bij de Commissie gebeuren. Evenwel voorziet artikel 55 van het koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens in een uitzondering voor verwerkingen die uitsluitend het klantenbeheer tot doel hebben (klantenkaart winkel). Deze uitzondering dient evenwel limitatief te worden geïnterpreteerd. Indien bijvoorbeeld het klantenbestand wordt aangewend om 'gebruikersprofielen' op te stellen, valt dit buiten het loutere klantenbeheer, en dient derhalve een aangifte bij de Commissie te gebeuren.

C. Opslagtermijn van de gegevens

30. De persoonsgegevens bekomen via de RFID toepassing en de bijkomende gegevens die het resultaat zijn van de omstandigheden van de inzameling zouden niet langer mogen bewaard worden dan noodzakelijk is voor de verwezenlijking van het geplande doeleinde[16].

31. Zo moeten bijvoorbeeld de tags op een product in de winkel (bedoeld voor stockbeheer) door de klant kunnen worden uitgeschakeld bij aankoop ervan (cfr. supra, punt 24), indien dit mogelijk is voor het specifieke product.

D. Veiligheidsmaatregelen

32. De verantwoordelijke voor de verwerking en desgevallend zijn verwerker, moeten de nodige technische en organisatorische veiligheidsmaatregelen[17] treffen om de RFID toepassing - waarin begrepen het systeem om het dataverkeer in te verwerken- en de daarmee verwerkte gegevens te beschermen tegen al dan niet toevallige vernietiging, tegen toevallig verlies, alsook tegen wijziging, toegang en iedere andere ongeoorloofde verwerking van

[16] Artikel 4, §1, 5° van de WVP.

[17] Artikel 16 van de WVP

persoonsgegevens. Hieromtrent verwijst de Commissie ter informatie naar de door haar opgestelde veiligheidsnormen welke volgens de Commissie, naargelang van geval tot geval,toepasbaar dienen te zijn op een verwerking van persoonsgegevens[18].

33. De Commissie beveelt aan de verantwoordelijken verder[19] aan om :

- Een 'privacy assessment' te doen inzake de implicaties van de RFID toepassing op de privacy en bescherming van persoonsgegevens, waaronder de vraag of de toepassing kan gebruikt worden voor de 'monitoring' van een persoon. Hoe hoger de privacyrisico's van een bepaalde toepassing, hoe hoger het niveau van de 'assessment' dient te zijn;
- Verantwoordelijken aan te duiden voor de opvolging van de 'assessments' en het nagaan van de efficiëntie van de technische en organisatorische veiligheidsmaatregelen; het is onontbeerlijk dat de verantwoordelijke voor de verwerking de technologische evoluties nauwgezet opvolgt teneinde de veiligheidsmaatregelen hierop af te stemmen[20].
- De 'assessment' ter beschikking te stellen van de toezichthoudende overheid, minstens zes weken voor de in gebruik name van de toepassing;

34. Overeenkomstig artikel 15 bis van de WVP kan de verantwoordelijke voor de verwerking verantwoordelijk gesteld worden voor de schade die zou te wijten zijn aan de niet-naleving of de inefficiëntie van de veiligheidsmaatregelen.

35. Tenslotte is er voor de industrie[21] een grote rol weggelegd met betrekking tot de veiligheidsmaatregelen en privacyvoorzieningen. Door de toepassing van zogenaamde 'security and privacy by design', wordt het voor de verantwoordelijken voor de verwerking veel eenvoudiger om te kiezen voor een privacy conform systeem. De Commissie is steeds bereid om met de sector hieromtrent samen te zitten voor advies.

(get.) Voor de Administrateur m.v., (get.) De Voorzitter,

Patrick Van Wouwe Willem Debeuckelaere

---

[18] http://privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

[19] Zie de aanbeveling van de Europese Commissie d.d. 12 mei 2009, o.c., punten 4-5;

[20] Artikel 16 van de WVP

[21] Zie de aanbeveling van de Europese Commissie d.d. 12 mei 2009, o.c., punt17;