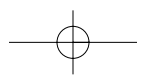
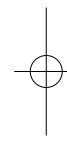
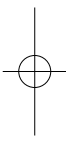


RFID & Privacy voor managers



RFID & Privacy voor managers

Een productie van:



Ministerie van Economische Zaken



Colofon

Dit boekje is deel twee in een serie over de toepassing van RFID binnen het bedrijfsleven, een initiatief van het Platform Detailhandel Nederland en het ministerie van Economische Zaken. De inhoud van deze publicatie is samengesteld door ECP.NL en het RFID Platform Nederland.

Teksten

Mr. Bart W. Schermer, ECP.NL/RFID Platform Nederland

Ontwerp omslag en binnenwerk:

ECP.NL / Efficiënta Offsetdrukkerij bv

Druk

Efficiënta Offsetdrukkerij bv

ISBN

90-76957-19-3

© 2006 Platform Detailhandel Nederland, ECP.NL, RFID Platform Nederland

Alle rechten voorbehouden. Niets uit deze uitgave mag worden veelevoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorgaande schriftelijke toestemming van de maker.

Alhoewel de auteurs en uitgever uiterste zorgvuldigheid betrachten bij het samenstellen van deze uitgave aanvaarden zij geen aansprakelijkheid voor schade van welke aard ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede) gebaseerd zijn op de in deze uitgave vervatte informatie. De wet- en regelgeving is een dynamisch terrein zodat de regels en richtlijnen die in deze uitgave worden genoemd inmiddels kunnen zijn veranderd.

Inhoudsopgave

1	Inleiding	5
2	Wat is RFID?	7
2.1	Hoe werkt RFID?	7
2.2	Soorten RFID	8
2.2.1	Productgebonden toepassingen	8
2.2.2	Persoonsgebonden toepassingen	8
2.3	Relevante privacyrechtelijke eigenschappen	8
3	Zorgen omtrent RFID & privacy	11
3.1	Het op afstand uitlezen van tags door readers	11
3.2	Volgbaarheid	11
3.3	Profilering van personen	12
3.4	Taggen van mensen	12
3.5	Misbruik	12
3.6	Het koppelen van systemen	13
4	Hoe om te gaan met privacy en RFID?	14
4.1	De Wet bescherming persoonsgegevens	14
4.2	Wat is een persoonsgegeven?	15
4.3	Wanneer is er bij RFID sprake van een persoonsgegeven?	15
4.4	Regels bij verwerken van persoonsgegevens	17
4.4.1	Eisen aan de gegevensverwerking	17
4.4.2	Verplichtingen als verantwoordelijke	19
4.5	Overige wet- en regelgeving	20
5	RFID en de consument	21
5.1	Openheid en transparantie	21
5.2	Informereren	22
5.3	Voorlichting	23
5.4	Keuzevrijheid	23
5.5	Toegevoegde waarde en service	24
5.6	Noodzakelijkheid	25

6	Inrichting van uw RFID-systeem	26
6.1	De keuze voor de juiste technologie	26
6.2	Koppeling	27
6.3	Informatiebeveiliging	27
6.4	Procedures	28
6.5	Hulp bij het inrichten van uw RFID-systeem	29
7	Conclusie	30
8	Meer weten?	31

1 Inleiding

Radio Frequency Identification technologie (RFID) mag zich in een grote belangstelling verheugen. Dit is ook niet zo verwonderlijk, want RFID gaat op tal van plaatsen in onze maatschappij, met name in de logistiek en detailhandel, voor grote veranderingen zorgen. RFID zal in belangrijke mate bijdragen aan de welvaart en veiligheid van onze maatschappij en de toepassing van RFID zal volgens kenners een grotere impact hebben op ons leven dan het internet dat heeft gehad.

U heeft waarschijnlijk al over RFID gehoord en wellicht bent u als ondernemer of beslisser reeds bezig om te kijken wat de mogelijkheden van RFID zijn voor uw organisatie. Naast de bedrijfseconomische aspecten van RFID dient u echter ook een aantal andere zaken mee te nemen in uw besluitvorming. RFID herbergt net als elke andere technologie namelijk bij verkeerd gebruik ook mogelijke risico's in zich. Hierbij gaat het dan met name om effecten van RFID op de privacy, gezondheid en het milieu. Een deel van de consumenten staat sceptisch tegenover RFID omdat zij zich zorgen maken over deze aspecten.

Consumenten maken zich bij het gebruik van RFID met name zorgen om hun privacy. Vragen over het milieu en de gezondheid staan minder hoog op de agenda.¹ Deze laatste twee onderwerpen zijn ook nog het voorwerp van wetenschappelijk onderzoek en in die zin is het nog onduidelijk of, en zo ja, wat voor gevolgen RFID heeft voor de volksgezondheid en het milieu.

Uit eerder onderzoek is gebleken dat bij onverantwoord gebruik van RFID inderdaad mogelijkheden zijn tot misbruik en dat dit mogelijk gevaar oplevert voor de privacy.² Echter, wanneer de wet wordt nageleefd, goede afspraken worden gemaakt en de consument goed wordt voorgelicht, dan is er geen reden tot

¹ Capgemini (2004). RFID and Consumers.

² ECP.NL (2005). Privacyrechtelijke Aspecten van RFID.

zorg. Het bedrijfsleven draagt daarbij een deel van de verantwoordelijkheid. Voor veel bedrijven is het echter onduidelijk hoe zij om moeten gaan met de privacyrechtelijke aspecten van RFID.

Om bedrijven te helpen bij een verantwoorde toepassing van RFID-technologie is deze brochure opgesteld. U krijgt een overzicht van de privacyrechtelijke aspecten van RFID die van belang zijn voor uw bedrijfsvoering. Allereerst wordt een korte beschrijving gegeven van wat RFID-technologie nu precies is, welke verschijningsvormen het heeft en welke toepassingen er zoal zijn. Vervolgens wordt gekeken wat de mogelijke risico's zijn bij het niet zorgvuldig toepassen van RFID. Aan de hand van de huidige privacywetgeving en enkele zelfreguleringsinitiatieven op het gebied van RFID wordt vervolgens gekeken wat de regels bij het gebruik van RFID zijn. Daarnaast worden suggesties gedaan over hoe u de acceptatie van de technologie door consumenten verder kunt stimuleren. Tot slot worden handreikingen gegeven voor een zorgvuldige inrichting van RFID-systemen binnen uw bedrijf.

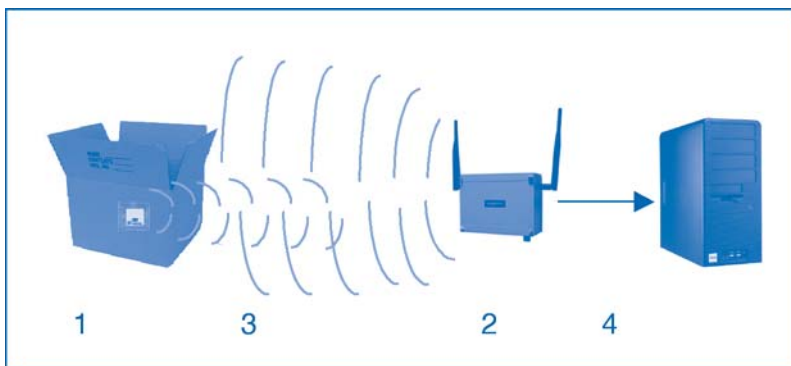
2 Wat is RFID?

RFID staat voor Radio Frequency Identification en is een technologie waarmee met behulp van *radiogolven* de unieke *automatische identificatie* van producten, dieren en personen op afstand mogelijk wordt gemaakt.

In dit hoofdstuk wordt slechts kort aangegeven hoe RFID-technologie werkt. Wilt u meer weten over de technologie in zijn algemeenheid en mogelijke toepassingsgebieden, raadpleeg dan deel 1 in deze serie: *RFID voor managers*.

2.1 Hoe werkt RFID?

RFID werkt als volgt: een op een object bevestigde chip gekoppeld aan een antenne (1), kan radiosignalen opvangen die worden uitgezonden door speciale leesapparaten (2). De chip gebruikt de elektromagnetische energie van het uitgezonden radiosignaal (3) om een bericht terug te sturen aan het leesapparaat. De inhoud van dit bericht is de informatie die opgeslagen ligt in de chip. Meestal is dit slechts een uniek nummer, maar er kan ook aanvullende informatie in de chip worden opgeslagen zoals productinformatie. Het leesapparaat stuurt deze informatie vervolgens door naar achterliggende informatieverwerkende systemen (4).



Schematische weergave van een RFID-systeem

2.2 Soorten RFID

RFID kent vele verschijningsvormen. De reden hiervoor is dat bepaalde typen RFID beter geschikt zijn voor bepaalde toepassingen dan anderen. Een onderscheid dat in het kader van RFID verhelderend kan werken is het onderscheid tussen productgebonden toepassingen en persoonsgebonden RFID-toepassingen.

2.2.1 Productgebonden toepassingen

Wanneer we spreken over productgebonden toepassingen dan hebben we het over de identificatie van producten en lastdragers (pallets, containers, dozen). In de categorie productgebonden toepassingen is de belangrijkste verschijningsvorm van RFID de Electronic Product Code (EPC) smart label. Daarnaast is er nog een veelvoud aan verschijningsvormen die speciaal toegesneden zijn op één bepaalde toepassing of omgeving. In dit kader spreken we dan van bedrijfs- of sectorspecifieke toepassingen.

2.2.2 Persoonsgebonden toepassingen

Bij persoonsgebonden RFID-toepassingen wordt RFID-technologie toegepast om personen te identificeren. Het gaat dan om het gebruik van zogenaamde tokens. Een token is een opslagmedium dat informatie bevat die gebruikt kan worden voor identificatie, authenticatie en autorisatie. Het gebruik van tokens is wijdverbreid in onze maatschappij, denk bijvoorbeeld aan het gebruik van bankpassen en toegangskaarten. Tot op heden maken tokens overwegend gebruik van 'contacttechnologie' zoals de magneetstrip of kaartlezer, maar contactloze tokens zijn aan een sterke opmars begonnen. Voorbeelden van deze laatste categorie zijn de OV-chipkaart en de contactloze werknemerspassen.

2.3 Relevante privacyrechtelijke eigenschappen

Net als veel andere nieuwe technologieën dat doen, roept RFID-technologie vragen omtrent de privacy van personen op. Veel van deze vragen hebben op zichzelf weinig met de technologie

RFID te maken. Hoe bijvoorbeeld door bedrijven met persoonsgegevens wordt omgesprongen is niet zozeer een RFID-vraagstuk, maar veeleer een organisatorisch vraagstuk (Hoe richt ik mijn databases in? Met wie deel ik de gegevens?). Toch roept de introductie van RFID een aantal specifieke aandachtspunten rondom privacy op. Deze aandachtspunten zullen in het volgende hoofdstuk nader besproken worden. Wat belangrijk is om te onderkennen is dat zij hoofdzakelijk voortvloeien uit een aantal specifieke technische eigenschappen die RFID-technologie heeft.

- *Leesgemak*

Omdat het met RFID zo makkelijk is om gegevens te verzamelen, is de kans groot dat er ook meer gegevens verzameld worden. Naarmate er meer informatie over personen wordt verzameld, worden vraagstukken rondom privacy relevanter.

- *Onzichtbaarheid*

Omdat RFID met onzichtbare radiogolven werkt is het niet noodzakelijkerwijs duidelijk wanneer een RFID-tag wordt uitgelezen. De 'onzichtbaarheid' van RFID draagt op deze manier bij aan mogelijke privacyvraagstukken.

- *Leesafstand*

Een belangrijke technische eigenschap van RFID is dat informatie op afstand draadloos uit te lezen valt. De maximale leesafstand van een RFID-toepassing is van grote invloed op mogelijke privacyrechtelijke vraagstukken. Naar mate de afstand groter wordt, worden privacyvraagstukken relevanter.

- *Afmeting*

De chip in een gemiddelde RFID-tag is niet veel groter dan een speldenknop en hoewel de antenne nog redelijk wat ruimte in beslag neemt, zijn RFID-tags toch heel klein. Door de geringe afmeting van RFID-tags kunnen ze gemakkelijk in producten worden verwerkt zonder dat dit direct zichtbaar is voor de consument.

- *Beveiliging*

Onbeveiligde RFID-tags geven hun informatie prijs aan elke RFID-lezer die in staat is om met de tag te communiceren, ongeacht het feit of de informatie op de tag ook daadwerkelijk voor de persoon in kwestie bedoeld is. Belangrijke kanttekening bij dit aandachtspunt is dat het heel goed mogelijk is om RFID-tags te voorzien van beveiliging indien dat nodig is.

3 Zorgen omtrent RFID & privacy

De unieke eigenschappen van RFID kunnen bij onzorgvuldig of onrechtmatig gebruik een inbreuk op de privacy veroorzaken. De zorg van critici is dan ook dat het gebruik van RFID-systemen afbreuk doet aan het recht op privacy. De reden hiervoor is dat de hoeveelheid persoonsgegevens die zonder wetenschap van de betrokkene kan worden verzameld groot zou kunnen zijn. Deze informatie zou kunnen worden aangewend om consumenten en werknemers te beïnvloeden of te controleren. In dit hoofdstuk worden enkele veel gehoorde bezwaren tegen RFID op een rij gezet.

3.1 Het op afstand uitlezen van tags door readers

Het ongemerkt en ongewenst uitlezen van RFID-tags wordt als het belangrijkste privacyrisico van RFID gezien. Doordat de kleine RFID-tags slim verwerkt worden in de verpakking van producten is het vaak moeilijk vast te stellen of een product een RFID-tag bevat. Dit gekoppeld aan het feit dat RFID-tags op afstand ongemerkt kunnen worden uitgelezen maakt het voor consumenten onduidelijk wie, wat, waar, hoe en wanneer over hen te weten komt aan de hand van de RFID-tags die zij bij zich dragen.

Een belangrijk aandachtspunt bij dit risico is de maximale leesafstand tussen reader en tag. Met andere woorden: welke reikwijdte heeft het radiosignaal en van welke afstand is het dus mogelijk RFID-tags uit te lezen. Het moge duidelijk zijn dat het risico voor de privacy groter is naarmate de leesafstand van de reader tot de tag toeneemt.

3.2 Volgbaarheid

RFID-systemen maken het in theorie mogelijk om mensen te volgen aan de hand van de RFID-tags die zij op of bij zich dragen. Dit probleem wordt relevanter op het moment dat verschillende RFID-systemen geïntegreerd worden tot een groter surveillance-

systeem. Het kunnen volgen van een individueel product vormt een risico voor de privacy op het moment dat het product te koppelen is aan een persoon. Op dat moment kan deze persoon namelijk in theorie gevolgd worden aan de hand van het artikel dat hij of zij bij zich draagt.

3.3 Profilering van personen

De hoeveelheid informatie die in potentie met een RFID-systeem verzameld kan worden is groot. Persoonlijke informatie verkregen met behulp van een RFID-systeem kan gebruikt worden om een individu te profileren. Deze informatie kan aangewend worden om een beter inzicht te krijgen in het gedrag van personen. Zo kan bijvoorbeeld onderscheid gemaakt worden tussen verschillende categorieën consumenten op basis van de verzamelde informatie.

3.4 Taggen van mensen

12 Naast producten kunnen ook mensen worden uitgerust met een RFID-tag. De RFID-tag kan worden aangebracht op een drager die een persoon bij zich draagt (bijvoorbeeld een kaart, sleutel of halsketting), of daadwerkelijk direct (onderhuids) op de persoon. Het taggen van mensen opent een groot spectrum aan controle mogelijkheden dat wellicht misbruikt kan worden. Zo kunnen mensen gevolgd worden, kan hen de toegang tot bepaalde locaties, goederen of diensten worden ontzegd en kan informatie ontleend aan de RFID-tag voor andere doeleinden worden aangewend.

3.5 Misbruik

Net als bij elke andere technologie (internet, telefonie) kan RFID ook worden misbruikt. Consumenten maken zich zorgen dat andere burgers met draagbare RFID-readers in hun boodschappenwagens, kleding of huis kunnen kijken. Consumenten voelen met name angst voor gerichte berovingen op basis van de informatie verkregen uit de RFID-tags.

3.6 Het koppelen van systemen

Een bedreiging die zich niet beperkt tot RFID maar zich uitstrekt tot alle systemen waarmee toezicht of controle kan worden uitgeoefend is het koppelen van systemen. Het koppelen van verschillende systemen zoals databases, camera's en RFID-systemen zou ervoor kunnen zorgen dat deze systemen tezamen veel effectiever worden, met andere woorden, het geheel is meer dan de som der delen.

4 Hoe om te gaan met privacy en RFID?

In het vorige hoofdstuk is een aantal zorgen over RFID-technologie onder de aandacht gebracht. Mogelijke privacyvraagstukken kunnen met name ontstaan wanneer RFID op een onzorgvuldige manier wordt toegepast, met andere woorden wanneer er bewust of onbewust in strijd met de privacywetgeving wordt gehandeld. In Nederland wordt het recht op privacy voornamelijk beschermd via de Wet bescherming persoonsgegevens.

4.1 De Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) regelt wat er wel en niet met persoonsgegevens mag gebeuren. De wet geldt voor de verwerking van gegevens van 'natuurlijke personen', een categorie waartoe consumenten behoren. Wanneer u dus gegevens van consumenten verzamelt en gebruikt dan is in veel gevallen de Wet bescherming persoonsgegevens van toepassing. Dit geldt voor het huidige gebruik van persoonsgegevens binnen uw onderneming en in de toekomst ook voor het gebruik van persoonsgegevens die met behulp van RFID zijn verzameld.

In deze publicatie zullen wij ons beperken tot het gebruik van persoonsgegevens in het kader van RFID-toepassingen. Daarom worden kort de verplichtingen uit de Wbp geschetst. Voor meer algemene informatie over de Wet bescherming persoonsgegevens kunt u zich wenden tot onder andere het College bescherming persoonsgegevens (de nationale toezichthouder op de Wet bescherming persoonsgegevens) en het ministerie van Justitie. Deze laatste heeft op haar website een *Handleiding voor de verwerking van persoonsgegevens* geplaatst, waarin u uitgelegd wordt hoe u als ondernemer om moet gaan met persoonsgegevens.

Voor meer informatie zie:

www.cbpweb.nl
www.justitie.nl

4.2 Wat is een persoonsgegeven?

Een persoonsgegeven is iedere informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). 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 specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit."* Om van een persoonsgegeven te kunnen spreken, moet de persoon op wie het gegeven betrekking heeft dus identificeerbaar zijn. Een persoon is identificeerbaar indien de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, is vast te stellen aan de hand van de gegevens die over deze persoon beschikbaar zijn.

Sommige gegevens verschaffen duidelijk feitelijke informatie over een persoon. De meest sprekende voorbeelden zijn iemands naam, geboortedatum of geslacht. Maar ook gegevens die niet direct betrekking hebben op een persoon (zoals bijvoorbeeld gegevens over objecten) kunnen onder omstandigheden persoonsgegevens zijn, mits de betrokkene identificeerbaar is. Of een gegeven over een object een persoonsgegeven is, hangt af van de context waarin het gegeven wordt verwerkt. Het gaat bij deze beoordeling met name om de vraag of de gegevens over het object, die gerelateerd zijn aan een persoon, mede bepalend is voor de wijze waarop deze persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Informatie over de medicatie die een persoon gebruikt zal bijvoorbeeld al snel een persoonsgegeven zijn indien deze informatie is terug te voeren op de betrokken persoon.

4.3 Wanneer is er bij RFID sprake van een persoonsgegeven?

Zoals in de vorige paragraaf reeds is aangegeven blijkt uit de Wet bescherming persoonsgegevens dat onder een persoonsgegeven wordt verstaan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. De informatie

die wordt verkregen uit een RFID-tag kan dus een persoonsgegeven zijn indien de informatie terug te voeren is op een geïdentificeerde of identificeerbare persoon. Een dergelijke situatie kan op de volgende manieren ontstaan:

Opslag van persoonsgegevens in de RFID-tag

De eerste mogelijkheid waarbij er vrijwel direct sprake is van de verwerking van persoonsgegevens als een RFID-tag wordt uitgelezen, is indien persoonsgegevens opgeslagen liggen in de RFID-tag zelf. Hierbij gaat dus niet om productgebonden toepassingen, maar juist om persoonsgebonden toepassingen. Afhankelijk van de gekozen toepassing (zoals beveiliging of zorg) kan het nuttig of noodzakelijk zijn persoonsgegevens (NAW gegevens, biometrische kenmerken) op te slaan in een RFID-tag om daarmee het proces van identificatie, authenticatie, en autorisatie te vergemakkelijken. De opslag van persoonsgegevens op een RFID-tag gebeurt met name op smartcards, implantaten en andersoortige tokens.

16 *Koppeling van persoonsgegevens aan informatie uit de RFID-tag*

De meeste smart labels en tags van bedrijfs- of sectorspecifieke systemen bevatten enkel een unieke code. Zo wordt in het EPCglobal Network enkel een unieke code opgeslagen op de tag. De unieke code die op een smart label wordt opgeslagen kan door de reader en middleware gekoppeld worden aan additionele productinformatie die ligt opgeslagen in een achterliggende database. Op dit moment is er nog geen sprake van een persoonsgegeven, de informatie is immers nog niet terug te voeren op een natuurlijke persoon.

Een koppeling komt pas tot stand op het moment dat de unieke productcode in de tag verbonden wordt aan de klant. In geval van een betaling in een supermarkt zou er dus sprake zijn van het verwerken van persoonsgegevens indien de supermarkt de gegevens omtrent de afgerekende producten koppelt aan de persoon die ze gekocht heeft, bijvoorbeeld door middel van een klantenkaart, betaling met creditcard, maar bijvoorbeeld ook door het koppelen van camerabeelden van de consument aan informatie uit RFID-tags.

4.4 Regels bij het verwerken van persoonsgegevens

Het is niet verboden persoonsgegevens te verwerken. In veel gevallen is het verwerken van persoonsgegevens zelfs noodzakelijk, bijvoorbeeld om een transactie te kunnen doen of een product te kunnen leveren. Wel moet er een goede grondslag zijn voor de verwerking van persoonsgegevens. Is een dergelijke grondslag niet aanwezig, of gebruikt u de gegevens voor een ander doel dan waarvoor zij oorspronkelijk zijn verkregen, dan is de verwerking in strijd met de wet. Daarnaast moet u als verantwoordelijke voor de gegevensverwerking voldoen aan een aantal verplichtingen.

4.4.1 Eisen aan de gegevensverwerking

Het gaat te ver om hier de gehele Wet bescherming persoonsgegevens uitgebreid te bespreken, daarom beperken wij ons tot de hoofdpunten van de wet. Deze zijn samen te vatten in enkele eisen die aan elke gegevensverwerking worden gesteld. De eisen zijn gericht aan de 'verantwoordelijke', de persoon of instantie die de verantwoordelijkheid draagt voor de verwerking.

- *Zorgvuldigheid (artikel 6 Wbp)*

De eerste eis betreft de zorgvuldigheid van de gegevensverwerking. Deze dient in overeenstemming met de wet en behoorlijk en zorgvuldig te gebeuren.

- *Grondslag voor de verwerking (artikelen 7 en 8 Wbp)*

Persoonsgegevens mogen alleen worden verwerkt indien hier een grondslag voor bestaat die duidelijk, uitdrukkelijk omschreven en gerechtvaardigd is. Grondslagen voor de verwerking zijn onder andere:

- de ondubbelzinnige toestemming van de betrokkene;
- de gegevensverwerking is noodzakelijk voor het uitvoeren van een overeenkomst waarbij de betrokkene partij is;
- de behartiging van het gerechtvaardigde belang van de verantwoordelijke.³

³ Bij deze laatste grondslag wordt het belang van de verantwoordelijke afgewogen tegen het belang van de betrokkene.

Voor uw bedrijfsvoering zijn deze grondslagen naar alle waarschijnlijkheid het meest relevant. Overige grondslagen vindt u in artikel 8 van de Wbp. Voor meer informatie kunt u de *Handleiding voor de verwerking van persoonsgegevens* raadplegen.

Wanneer u een RFID-systeem (mede) gaat gebruiken voor het verwerken van persoonsgegevens, dan dient u de doeleinden van de verwerking dus welbepaald en uitdrukkelijk te omschrijven en moet u zich kunnen beroepen op één van de grondslagen van de wet. Het zonder direct doel verzamelen van persoonsgegevens is in strijd met de wet.

- *Doelbinding (artikel 9 Wbp).*

Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden van de originele verkrijging. Met andere woorden, gegevens die met het oog op een bepaald doel zijn verzameld mogen niet zomaar voor een ander doel worden aangewend. Welke eisen worden gesteld aan de doelbinding kunt u nalezen in de *Handleiding voor de verwerking van persoonsgegevens*.

- *Bewaren gegevens (artikel 10 Wbp)*

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het uitvoeren van het vooraf gespecificeerde doel. U mag dus verzamelde gegevens niet bewaren indien u geen doel meer heeft voor de verwerking.

- *Kwaliteit (artikel 11 Wbp)*

Persoonsgegevens mogen slechts worden verwerkt indien zij met het oog op het doel van de verwerking toereikend, ter zake dienend en niet bovenmatig zijn. Daarnaast moeten de gegevens juist en nauwkeurig zijn.

- *Beveiliging (artikelen 12, 13 en 14 Wbp)*

Wanneer u persoonsgegevens verwerkt, dan dient u zorg te dragen voor een adequate beveiliging. Wanneer u gebruik maakt van een RFID-systeem dat gebruikt wordt om persoonsgegevens te verzamelen en te verwerken dan moet u zorgen dat alle relevante delen van het systeem beveiligd zijn. Dit is met name van belang wanneer op de RFID-tag zelf persoonsgegevens opgeslagen zijn. In dit geval moeten naast de ach-

terliggende databases namelijk ook de tag en het overgebrachte signaal beveiligd zijn.

4.4.2 Verplichtingen als verantwoordelijke

Als verantwoordelijke voor de verwerking van persoonsgegevens heeft u een aantal plichten bovenop de eisen die aan de verwerking van persoonsgegevens wordt gesteld. Het betreft de volgende plichten:

Informereren van de betrokkene

U dient de betrokkene te informeren indien u persoonsgegevens van hem of haar verwerkt. U moet de betrokkene informeren over wie u bent en met welk doel u voornemens bent gegevens te gaan verwerken. U dient de betrokkene hierover vooraf te informeren.

Dit vereiste is met name bij het gebruik van RFID van bijzonder groot belang, omdat de betrokkene veelal niet zal merken wanneer (persoons)gegevens worden uitgelezen met behulp van RFID. Wanneer u RFID gaat gebruiken dan doet u er goed aan de consument hierover te informeren, bijvoorbeeld door te melden dat het product een RFID-tag bevat en aan te geven waar RFID-readers geplaatst zijn.

Melding bij het College bescherming persoonsgegevens

Wanneer u voornemens bent gegevens te gaan verwerken, dan dient u dit in bepaalde gevallen te melden bij de nationale toezichthouder, het College bescherming persoonsgegevens of een door uw branche aangewezen functionaris. In welke gevallen u de gegevensverwerking moet melden bij het College of de functionaris kunt u nalezen op de website van het College.

Inzage en correctie

Degene wiens gegevens u verwerkt heeft recht op inzage in de gegevens die u van hem of haar verwerkt en u moet dus verzoeken tot inzage honoreren. Daarnaast kan de betrokkene u vragen zijn of haar gegevens te corrigeren. Hieronder valt aanvullen, verbeteren, afschermen en verwijderen.

4.5 Overige wet- en regelgeving

De Wet bescherming persoonsgegevens is een algemene wet op het gebied van de privacy. Het kan zijn dat voor uw bedrijfsvoering of specifieke toepassing van RFID nog aanvullende wetten, regels of afspraken gelden. Het voert echter te ver om in deze brochure allerlei sectorspecifieke regulering te bespreken. Indien u niet zeker weet of voor uw bedrijfsvoering of specifieke toepassing nog aanvullende regels gelden, dan kunt u zich het beste wenden tot uw branchevereniging of tot een gespecialiseerd jurist.

Voor een overzicht van gespecialiseerde IT juristen kunt u op de website van ECP.NL (www.ecp.nl), platform voor eNederland, kijken onder het dossier 'juristenpool'.

Naast wetgeving vanuit de overheid op het gebied van de bescherming van de privacy zijn er ook een aantal (internationale) zelfreguleringsinitiatieven vanuit de markt op het gebied van RFID. Deze initiatieven hebben tot doel de wetgeving in het kader van RFID te verduidelijken en de acceptatie van RFID door de consument te helpen stimuleren. In de bijlagen van deze brochure vindt u een nadere toelichting op twee belangrijke zelfreguleringsinitiatieven: *de ICC principles on EPC deployment and operation* en de *EPCglobal Guidelines*.⁴

De belangrijkste regels die naar voren komen uit beide documenten zijn:

- (1) het informeren van de consument,
- (2) het voorlichten van de consument,
- (3) het bieden van vrije keuze aan de consument,
- (4) het naleven van bestaande wetgeving en
- (5) het zorgen voor een goede beveiliging van gegevens.

In feite betreft het hier vergelijkbare regels als die voortvloeien uit de Wet bescherming persoonsgegevens.

⁴ U kunt de volledige richtlijn raadplegen en downloaden via de International Chambers of Commerce website: <http://www.iccwbo.org/id600/index.html>. De volledige EPCglobal Guidelines kunt raadplegen via de EPCglobal website: http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

5 RFID en de consument

De in de Wet bescherming persoonsgegevens genoemde vereisten en verplichtingen bij het verwerken van persoonsgegevens, vormen slechts een deel van het verhaal rondom RFID en privacy. Het gaat namelijk bij het gebruik van RFID niet enkel om het voldoen aan wettelijke regels, maar juist om de acceptatie van de technologie door de consument. Wanneer deze, ondanks dat u aan alle wettelijke verplichtingen voldoet, toch een ongemakkelijk gevoel krijgt bij uw RFID-toepassingen, dan kost dit u mogelijk klandizie en schaadt het de ontwikkeling van RFID in Nederland. De mening van de consument is dus uiteindelijk minstens zo belangrijk als de wettelijke regels. Als ondernemer dient u hier terdege rekening mee te houden.

U kunt op diverse manieren de consument tegemoet komen en zorgen voor een verantwoorde toepassing van RFID die de consument ook nog eens toegevoegde waarde biedt. Hieronder zijn enkele belangrijke aandachtspunten opgenomen waarmee u rekening moet houden.

21

5.1 Openheid en transparantie

Omdat RFID een 'onzichtbare' technologie is, is het belangrijkste aandachtspunt bij het gebruik van RFID de zorg voor openheid en transparantie. Door het onzichtbare aspect van de technologie kunnen consumenten potentieel de controle over hun gegevens verliezen, omdat zij niet langer degenen zijn die bepalen wanneer hun persoonsgegevens worden prijsgegeven. Dit maakt het dat RFID een technologie is waar consumenten kritisch naar kijken. Het laatste dat u in dit soort gevallen wilt is geheimzinnig of gesloten zijn over het gebruik van RFID binnen uw onderneming. Dergelijk gedrag werkt immers argwaan in de hand.

Zelfs als het gebruik van RFID niets te maken heeft met het verwerken van persoonsgegevens kunnen spookverhalen uit andere branches en ondernemingen uw RFID-implementatie onterecht verdacht maken. Openheid en transparantie vanuit uw

kant zorgt ervoor dat dergelijke verhalen ontkracht worden en klanten met een gerust hart de weg naar uw onderneming vinden.

Zorg er daarom voor dat u uw klanten betreft bij uw RFID-implementaties, op zijn minst door open en transparant op vragen te reageren of nog liever, door bij uw klanten na te gaan wat hun wensen, voorkeuren en angsten op het gebied van RFID zijn.

5.2 Informeren

Het informeren van de consumenten waar RFID-tags zich in uw producten bevinden en waar u RFID-readers heeft geplaatst is een verplichting die voortvloeit uit onder andere de Wet bescherming persoonsgegevens en zelfregulering op het gebied van RFID. Maar zelfs wanneer u géén persoonsgegevens verwerkt met behulp van RFID is het tóch van belang om de consument te informeren over het gebruik ervan. Op deze manier vergroot u het vertrouwen van de consument in uw onderneming en in het gebruik van RFID-technologie.

U kunt uw klanten op verschillende manieren attenderen op het gebruik van RFID. Door middel van een duidelijk beeldmerk kunt u bijvoorbeeld aangeven dat een product een RFID-tag bevat. U kunt verder de locatie van RFID-readers aanduiden met behulp van onder andere bordjes, stickers of een plattegrond. Mochten deze maatregelen niet mogelijk zijn, dan moet u in ieder geval melding maken van het feit dat binnen uw onderneming gebruik wordt gemaakt van RFID.

Als aanvulling op deze informatie zou u uw klant ook nog een korte brochure ter beschikking kunnen stellen met daarin een korte uitleg over de door u gebruikte RFID-toepassing en uw 'RFID-beleid'. U kunt ook op uw website aanvullende informatie beschikbaar stellen en eventueel verwijzen naar andere websites met informatie over RFID.

5.3 Voorlichting

In samenhang met de plicht om uw klant te informeren over het gebruik van RFID binnen uw onderneming is het ook wijs uw klant voor te lichten over RFID in zijn algemeenheid. Hierbij zijn samenwerkingsverbanden (bijvoorbeeld op brancheniveau) de beste methode om zoveel mogelijk consumenten te bereiken.

Over RFID-technologie bestaan veel misverstanden en consumenten hebben veelal een onrealistisch beeld van de mogelijkheden en onmogelijkheden van RFID. De mogelijkheden van verschillende typen RFID lopen behoorlijk uiteen. Maar de consument maakt geen onderscheid tussen verschillende typen RFID, zij onderscheiden slechts de term RFID. Er bestaan met name veel misverstanden over de maximale leesafstanden van RFID en de interoperabiliteit (koppeling) van RFID-systemen.

Wat echter wel of niet waarheid is in technische zin doet minder ter zake dan het uitleggen wat uw concrete toepassing van RFID-technologie is. Het is dus niet voldoende enkel de technische specificaties van uw RFID-systeem uit de doeken te doen. U moet ook uitleggen wat u wel en niet met de verzamelde informatie doet en hoe u deze informatie beveiligt.

5.4 Keuzevrijheid

Keuzevrijheid voor de consument speelt een belangrijke rol bij de acceptatie van RFID. Zo mag de consument door het gebruik van RFID niet worden gedwongen om onvrijwillig persoonsgegevens prijs te geven. Maar naast deze wettelijke verplichting kan de consument ook uit andere overwegingen bezwaar hebben tegen het gebruik van RFID in producten. Het is daarom zaak de consument zoveel mogelijk keuzevrijheid te geven bij het gebruik van RFID.

Hoe deze keuzevrijheid voor de consument vormgegeven moet worden, is nog onderwerp van debat. De consument kan allereerst een keuze worden gegeven door hem of haar de optie te geven een RFID-tag te deactiveren (de zogenaamde KILL

feature) of te verwijderen. Een andere mogelijkheid, die nog meer zekerheid biedt voor de consument is het deactiveren van de RFID-tag op het moment dat het product in de schappen ligt. Het kan echter zo zijn dat wanneer de RFID-tag uiteindelijk als radio-barcode wordt gebruikt dit geen optie meer is.⁵

In ieder geval moet de consument altijd de mogelijkheid geboden worden om van deze optie gebruik te maken, tenzij er zwaarwegende redenen zijn om de optie niet te bieden. De keuze voor het deactiveren moet niet onredelijk bezwarend zijn voor de consument, deze moet namelijk niet met 'zachte hand' gedwongen worden om de tag actief te laten. Zo wordt door consumentenorganisaties aangegeven dat zij lange rijen bij het deactiveren beschouwen als een onvrije keuze. Een voorbeeld van een onvrije keuze die in strijd is met het recht, is het enkel bieden van garantie als de RFID-tag actief blijft.

5.5 Toegevoegde waarde en service

24

Uit onderzoek is gebleken dat de consument in Nederland niet per definitie negatief tegenover RFID staat. In tegendeel, een groot deel van de Nederlandse consumenten ziet veel voordelen in het gebruik van RFID-technologie. Echter, de voordelen die u als ondernemer van belang vindt, doen voor een consument vaak veel minder ter zake. Een voorbeeld ter illustratie: veel bedrijven zien op maat gesneden marketing met behulp van RFID (narrowcasting) als één van de grootste voordelen van RFID; consumenten daarentegen zien dit als het minst belangrijke, sterker nog, velen zien het als een bedreiging van hun privacy. Wilt u dus de goede kanten van RFID benadrukken voor uw klant, dan zult u in de huid van de consument moeten kruipen en *niet* redeneren vanuit de voordelen die RFID biedt voor uw onderneming.

⁵ Het betreft hier een moeilijke discussie waar het laatste woord nog niet in gesproken is. Moet de consument namelijk een actieve handeling verrichten om de tag uit te schakelen (opt-out), of moet de RFID-tag per definitie uit staan in de winkel en heeft de consument de mogelijkheid deze op zijn verzoek te laten activeren (opt-in)?

Consumenten zijn voornamelijk geïnteresseerd in de manier waarop producten met RFID veiliger en goedkoper kunnen worden gemaakt. Consumenten zijn bijvoorbeeld erg geïnteresseerd in de mogelijkheden van RFID voor het sneller terugvinden van gestolen goederen zoals auto's en digitale camera's. Ook verbeterde veiligheid van medicatie en voedingsmiddelen zijn voordelen die de consument ziet in RFID. Tot slot willen de consumenten besparingen die bedrijven maken met RFID terugvinden in de prijs van hun producten.

Wanneer u dus naast de wettelijke waarborgen die u moet bieden, de voordelen van RFID kunt vertalen naar voordelen voor de consument, dan zal de acceptatie door de consument een stuk eenvoudiger zijn.

5.6 Noodzakelijkheid

Een zeer belangrijke vraag die u zichzelf moet stellen bij het gebruik van RFID is de volgende: is het nodig dat ik persoonsgegevens verwerk met behulp van een RFID-systeem? Wanneer er voor uw bedrijfsvoering geen noodzaak of toegevoegde waarde bestaat voor de verwerking van persoonsgegevens, doe het dan niet! U bespaart zichzelf een hoop kosten, moeite, negatief consumenten-sentiment en wellicht juridische gevolgen, wanneer u RFID niet gebruikt om persoonsgegevens te verwerken.

6 Inrichting van uw RFID-systeem

Op basis van wat hiervoor is beschreven, worden in dit hoofdstuk een aantal aandachtspunten aangedragen waarmee u rekening moet houden bij de inrichting van een RFID-systeem. Waar mogelijk worden concrete suggesties gedaan voor een optimale inrichting van uw RFID-systeem.

6.1 De keuze voor de juiste technologie

Wanneer u een RFID-systeem besluit in te richten dan doet u dit omdat u uw bestaande bedrijfsprocessen efficiënter kunt maken met behulp van RFID, met RFID een specifiek probleem kunt oplossen, of RFID nieuwe mogelijkheden biedt voor uw bedrijfsvoering. De businesscase en de *return on investment* die deze businesscase heeft zijn hierbij uiteraard leidend en dicteren de gekozen hardware en software. Maar wanneer uw RFID-toepassing de consument raakt, dan zult u ook deze factor moeten meewegen in uw beslissing voor de keuze van de technologie. De reden hiervoor is dat de gekozen technologie zijn weerslag heeft op eventuele privacyvraagstukken.

26

De belangrijkste keuze bij de inrichting van een RFID-systeem is de keuze voor het te gebruiken type RFID-technologie. Deze keuze zal allereerst afhangen van het doel van het RFID-systeem en de omgeving waarin het moet draaien. Zo functioneert een passieve UHF-tag bijvoorbeeld minder goed in een omgeving met veel metaal en daarom is deze toepassing minder geschikt voor het volgen van containers. Maar naast omgevingsfactoren speelt ook de vraag of er wel of niet persoonsgegevens in de RFID-tag worden opgeslagen een rol bij de keuze van een RFID-systeem. Wanneer u namelijk persoonsgegevens wilt opslaan in de tag (bijvoorbeeld voor een betaaltoepassing) dan zult u een RFID-tag moeten kiezen die in voldoende mate beveiligd kan worden en niet over grote afstand is uit te lezen.

Binnen de logistiek en detailhandel zullen naar alle waarschijnlijkheid drie toepassingen van RFID domineren: de toepassing van EPC smart labels (productgebonden), het gebruik van RFID in

loyaltycards (persoonsgebonden) en het gebruik van RFID/ NFC betaaltoepassingen (persoonsgebonden). Bij de eerste zult u gebruik moeten maken van de standaard EPC smartlabels en is het verstandig er zorg voor te dragen dat uw systeem de 'KILL feature' ondersteunt. Bij de laatste twee toepassingen zult u, wanneer persoonsgegevens op de tag worden opgeslagen, moeten kiezen voor een RFID-tag met een adequaat beveiligingsniveau.

6.2 Koppeling

Zoals aangegeven in hoofdstuk 3 kan de koppeling van systemen en gegevensverzamelingen extra privacyvraagstukken opleveren. Wanneer u besluit om verschillende systemen en gegevensverzamelingen met elkaar te koppelen dan dient u goed na te gaan of dit verenigbaar is met de regels uit de Wbp. U kunt hiertoe het College bescherming persoonsgegevens om advies vragen.

6.3 Informatiebeveiliging

27

Bij elk informatieverwerkend systeem, zeker als dit systeem bedoeld is om persoonsgegevens te verwerken, is beveiliging een belangrijk onderwerp. Zorg dragen voor een adequaat niveau van beveiliging is zelfs een wettelijke verplichting die voortvloeit uit de Wet bescherming persoonsgegevens. Bij RFID-systemen zal zorg gedragen moeten worden voor de beveiliging van drie afzonderlijke delen van het systeem: de RFID-tag, de overdracht van het signaal van de tag naar de reader en de achterliggende databases.

Beveiliging van de RFID tag

Wanneer slechts een uniek nummer op de tag wordt opgeslagen, zoals het geval is bij een productgebonden toepassing als de EPC smart label, dan is het veelal niet noodzakelijk om de tag van een beveiliging te voorzien. Wanneer u persoonsgegevens of andere belangrijke gegevens opslaat op de RFID-tag zelf, dan zult u deze tag moeten voorzien van adequate beveiliging (encryptie) om ervoor te zorgen dat de tag niet door onbevoegden wordt uitgelezen.

Beveiliging van het overgebrachte signaal

Het is mogelijk om radiosignalen met behulp van een radio-ontvanger af te vangen. Wanneer het overgebrachte signaal niet door middel van encryptie is versleuteld, dan kan elke onbevoegde derde met de juiste middelen kennis nemen van de inhoud van de overgebrachte boodschap. Wanneer dus gevoelige informatie wordt overgebracht zoals persoonsgegevens of toegangscode's, is het zaak naast de tag zelf, ook het overgebrachte signaal te versleutelen. Wanneer het gaat om productinformatie zoals bijvoorbeeld het geval is bij het gebruik van EPC smart labels, dan is encryptie van het radiosignaal veelal niet noodzakelijk, omdat de overgebrachte informatie niet gevoelig is (het betreft immers slechts een unieke code voor een product).

Beveiliging van achterliggende databases

Het spreekt voor zich dat ook de database waar de RFID-gegevens uiteindelijk in worden opgeslagen adequaat beveiligd moet zijn. Het betreft hier echter een situatie die niet specifiek geldt voor RFID: elke database waarmee (persoons)gegevens worden verwerkt moet voorzien zijn van beveiliging. De wijze waarop de informatie in het systeem is gekomen is in die zin niet relevant.

6.4 Procedures

Naast een adequaat niveau van informatiebeveiliging is het ook zaak om de procedures rondom het raadplegen, doorsturen en delen van (persoons)gegevens goed op orde te hebben. Het gaat dan voornamelijk om het goed vormgeven van identificatie-, authenticatie- en autorisatieprocedures. Dergelijke procedures zijn van belang omdat niet iedereen zomaar toegang kan of mag hebben tot uw gegevens. Dit geldt niet alleen voor derden (andere bedrijven), maar ook voor het eigen personeel. Het betreft hier hoofdzakelijk de inrichting van de achterliggende databases. Dit is echter geen RFID-specifiek onderwerp en zal daarom verder buiten beschouwing worden gelaten.

6.5 Hulp bij het inrichten van uw RFID-systeem

Bij de inrichting van een RFID-systeem is het vaak zinvol om een gespecialiseerde partij in te schakelen die er zorg voor draagt dat alle verschillende delen van uw RFID-systeem op elkaar afgestemd zijn (tags, readers, software) en alle noodzakelijke veiligheidsmaatregelen getroffen worden. Dergelijke partijen, ook wel 'system integrators' genoemd, kunnen u ook helpen bij de keuze voor een RFID-systeem dat rekening houdt met de privacy van de consument.

Indien u een kleinere onderneming heeft, of daarvoor werkzaam bent en geen budget voor een gespecialiseerde system integrator heeft, dan kunt u het beste een kant-en-klare RFID-oplossing kiezen.

Meer informatie over system integrators kunt u vinden op de website van het RFID Platform Nederland:
www.rfidnederland.nl

7 Conclusie

Het duurt waarschijnlijk nog wel enige tijd voordat uw klant in aanraking komt met RFID. Toch is het zinvol om nu al na te denken over de privacyrechtelijke aspecten van RFID. Bij de uiteindelijke inrichting van uw RFID-systeem zult u keuzes moeten maken die invloed hebben op de privacy van de consument. Een doordachte en verantwoordelijke toepassing van RFID beschermt niet alleen uw klant, maar kan ook uw onderneming een hoop voordeel opleveren. Wanneer u de consument voordelen en toegevoegde waarde biedt kan RFID juist een punt zijn waarmee u zich van uw concurrent kunt onderscheiden. Het is deze laatste overweging die leidend moet zijn in uw RFID-implementaties. U dient zichzelf daarom de volgende vraag te stellen: hoe zorg ik ervoor dat ik met RFID mijn onderneming en mijn klanten toegevoegde waarde bied.

8 Meer weten?

Wilt u meer weten over RFID of de privacyrechtelijke aspecten van RFID, dan kunt u (onder andere) bij de volgende bronnen terecht.

Platform Detailhandel Nederland

Postbus 262

2260 AG Leidschendam

T: 070-3202345

F: 070-3278797

W: www.platfordetailhandel.nl

RFID Platform Nederland

Postbus 262

2260 AG Leidschendam

T: 070-3376102

F: 070-4190650

W: www.rfidnederland.nl

ECP.NL, Platform voor eNederland

Postbus 262

2260 AG Leidschendam

T: 070-4190309

F: 070-4190650

W: www.ecp.nl

