

Universiteit Twente



*Bacheloropdracht*

De veranderingen door de RFID technologie bij Selexyz

---

BGN ICT

---



---

Hans van Veen (S0093734)

Universiteit Twente, Faculteit Management en Bestuur

Opleiding Bestuurskunde

## Opdrachtinformatie

De bacheloropdracht wordt uitgevoerd in opdracht van Selexyz.

Geplande stageperiode van de bacheloropdracht: 16 april tot en met 24 juni.

Informatie stagebedrijf: Selexyz, BGN ICT b.v.  
Maagdenburgstraat 16, 7421 ZC Deventer  
Postbus 357, 3990 GD Houten  
Telefoon: 030 6394090  
[www.Selexyz.nl](http://www.Selexyz.nl)

Begeleiders Selexyz: Dhr. Jan Veninga, Systeem analist/ontwikkelaar BO  
Telefoon: 06 47228789  
Email: [jveninga@bgn.nl](mailto:jveninga@bgn.nl)

Mw. Alette Zandbergen, Manager HRD  
Telefoon: 06 47228787  
Email: [azandbergen@bgn.nl](mailto:azandbergen@bgn.nl)

Begeleiders Universiteit Twente: Dr. Peter Schuur  
Telefoon: Tel: (053-489)3658/3912  
Email: [p.c.schuur@utwente.nl](mailto:p.c.schuur@utwente.nl)

Dr. Hans Heerkens  
Telefoon: (053-489) 3492  
Email: [j.m.g.heerkens@utwente.nl](mailto:j.m.g.heerkens@utwente.nl)

## **Inhoudsopgave**

<b>Voorwoord</b>	<b>Blz 5</b>
<b>1. Inleiding</b>	
1.1 Over Selexyz en de RFID technologie	Blz 6
1.2 De RFID technologie	Blz 8
<b>2. Onderzoeksopzet</b>	
2.1 Onderzoeksdoel	Blz 10
2.2 Onderzoeksvragen	Blz 11
2.3 Plan van aanpak	Blz 13
<b>3. Wat zijn de voordelen die de consumenten zien als Selexyz de RFID technologie invoert?</b>	
3.1 Voordelen die de consumenten zien	Blz 16
3.2 Voordelen rangschikken op belangrijkheid	Blz 18
3.3 Conclusie	Blz 20
<b>4. Wat kunnen de bezwaren van de klanten tegen de RFID technologie zijn?</b>	
4.1 Case Wal-Mart	Blz 21
4.2 Bezwaren RFID in Nederland	Blz 22
4.3 Relativeringen bij privacyrisico's	Blz 24
4.4 Conclusie	Blz 25
<b>5. Wat zijn de wettelijke restricties?</b>	
5.1 Overzicht Europese richtlijnen	Blz 28
5.2 De Wet Bescherming Persoonsgegevens	Blz 29
5.3 De Telecommunicatiewet	Blz 31
5.4 Conclusie	Blz 31
<b>6. Wat zijn de randvoorwaarden bij de invoeringswijze van RFID?</b>	
6.1 Waar moet Selexyz rekening mee houden, en wat kan Selexyz het beste doen om de invoering van de RFID technologie zo voorspoedig mogelijk te laten verlopen?	Blz 33
6.2 Conclusie	Blz 36

<b>7. Een communicatieplan voor Selexyz</b>	
7.1 Manieren om consumentengedrag te beïnvloeden	Blz 37
7.2 Adviezen	Blz 38
7.3 Oplossingsrichtingen voor Selexyz	Blz 40
<b>8. Literatuurlijst</b>	Blz 42
<b>Bijlagen</b>	
1. Internationale wetgeving (algemeen)	Blz 45
2. Regelgeving informatiele privacy	Blz 45
3. RFID specifieke (zelf)regulering	Blz 47
4. Voorgestelde RFID specifieke wetgeving	Blz 48
5. belangrijkste punten uit de Richtlijn 95/46/E	Blz 50
6. belangrijkste punten uit de Richtlijn 2002/58/EG	Blz 52
7. Alle histogrammen AHP	Blz 54
8. Exacte percentages AHP	Blz 55
9. Reflectieverslag	Blz 56
10. Samenvatting	Blz 59

## Voorwoord

Voor u ligt de opdracht die ik heb gemaakt om de bachelorfase van de studie bestuurskunde aan de Universiteit Twente af te ronden. Zo is het de bedoeling dat er onder begeleiding een empirisch onderzoek of een praktijkgerichte ontwerpopdracht uitgevoerd wordt. De bacheloropdracht zal in dit geval extern plaatsvinden. Selexyz is hier de externe opdrachtgever. De Universiteit Twente werd echter het meest als thuisbasis gebruikt. De opdracht wordt afgesloten met een schriftelijk rapport, een reflectieverslag en een presentatie in een colloquium.

In deze opdracht is het de bedoeling de expertise toe te passen die ik tijdens mijn studie heb opgedaan.

De opdracht is uitgevoerd in opdracht van Selexyz. De begeleider van Selexyz was mevrouw Alette Zandbergen. Dit is halverwege de opdracht, in week 20, veranderd aangezien ze stopte met haar werkzaamheden voor Selexyz. De heer Jan Veninga heeft vanaf toen de begeleiding op zich genomen. De begeleiders van de Universiteit waren de heer Peter Schuur en de heer Hans Heerkens.

Selexyz heeft me gevraagd een onderzoek te doen naar, zoals de titel al wel doet vermoeden, de veranderingen die door de RFID technologie bij Selexyz zullen komen. De RFID technologie is een technologie die een grote toekomst voorspeld wordt. Er wordt verwacht dat er grote economische voordelen met de technologie te behalen zijn. Maar daarnaast is de RFID technologie ook een omstreden technologie. In een land als de Verenigde Staten stuit de toepassing van de RFID technologie op grote weerstand onder de bevolking. Het is daarom niet ondenkbaar dat de RFID technologie in Nederland ook op weerstand zal stuiten.

Selexyz wil graag te weten komen óf er weerstand in Nederland zal ontstaan mocht Selexyz de RFID technologie op grotere schaal invoeren. En mocht er weerstand ontstaan, wat zijn dan de beste manieren om hier mee om te gaan.

Het is uiteindelijk een onderzoek geworden dat zowel voor Selexyz als voor de Universiteit Twente van waarde is. Dat wil zeggen een verslag waar Selexyz echt iets aan heeft in haar vraagstukken rond de RFID technologie en een verslag dat de naam van de Universiteit hoog houdt.

Enschede, 17 september 2007

## 1. Inleiding

### *1.1 Over Selexyz en de introductie van de RFID technologie*

Selexyz is een onderdeel van Boekhandels Groep Nederland, de grootste verkoper van boeken in Nederland. BGN heeft 16 consumentenwinkels in de grote steden en 26 boekwinkels nabij universiteiten of HBO-instellingen. Jaarlijks bezoeken meer dan 11 miljoen mensen één van de winkels van BGN en ze verkopen ongeveer 7 miljoen boeken aan meer dan 4 miljoen klanten.

Omdat de boekenprijs voor Nederlandstalige boeken wettelijk geregeld is, moet BGN speciale aandacht besteden aan de service voor klanten, assortiment en beschikbaarheid van titels en klantbeleving. Andere belangrijke onderwerpen binnen de organisatie hebben betrekking op het in de hand houden van kosten en het toepassen van innovatie. Er bestaat binnen BGN Selexyz (in het vervolg van het verslag zal ik BGN Selexyz voor het gemak Selexyz noemen) al langere tijd interesse voor de toepassing van RFID. Radio frequency identification (RFID) is een technologie om van een afstand informatie op te slaan en te lezen van zogenaamde RFID-tags die op of in objecten zitten (Min. EZ. 2006). Dit onderwerp staat al vanaf 2003 op de agenda. Na het treffen van de nodige voorbereidingen werd op 28 december 2005 definitief besloten de nieuwe selexyz boekwinkel in Almere, Selexyz Scheltema, in te richten op basis van RFID-technologie op item level. Ieder boek werd voorzien van een eigen unieke RFID-tag.

Vervolgens werd in november 2006 Selexyz Dominicanen in Maastricht geopend. Ook deze winkel is ingericht op de RFID technologie.

De RFID tags worden niet door Selexyz zelf op de boeken geplaatst. Dit is door hen uitbesteed aan het Centraal Boekhuis (CB). Het CB verzorgt de logistieke afwikkeling van het orderproces en de levering van artikelen.

Selexyz ziet voordelen bij de toepassing van de RFID technologie in haar winkels. Zo kunnen nooit alle boeken aanwezig zijn die de klant wil hebben. Door een sneller en simpeler bestelproces denkt Selexyz de service voor de klant te vergroten. Klanten kunnen nu zelf de boeken bestellen die ze willen hebben. Dit kan in de boekwinkel op een computerscherm of via internet. Als de klant het op prijs stelt kan er zelfs een sms naar de mobiele telefoon verstuurd worden als het desbetreffende boek bij Selexyz binnen is gekomen. Ook het zoekstelsel in de winkels wordt simpeler. Op het zoekscherm van een computer kan met een titel intypen en vervolgens wordt weergegeven in welk schap een boek staat dat gezocht wordt.

Daarnaast heeft RFID voor Selexyz zelf ook voordelen. Alle items zijn voorzien van een tag. Vanaf ontvangst van de goederen tot aan verkoop wordt gebruik gemaakt van RFID-technologie.



*Afbeelding 1: Het logistieke proces d.m.v. de RFID technologie*

De bestelde boeken komen binnen in dozen bij Selexyz. Deze hoeven niet meer uitgepakt te worden om te kijken of alle bestelde titels wel aanwezig zijn. De titels kunnen gescand worden. De boeken gaan in een doos door een tunnel heen en zo kan meteen bekeken worden of alle bestelde boeken aanwezig zijn. Dit scheelt een hoop tijd. Alle dozen hoeven nu niet meer uitgepakt te worden. Vervolgens worden de boeken in de winkel geplaatst. Boeken kunnen eenvoudig gezocht worden en er kan daarnaast ook makkelijk gekeken worden hoeveel en welke boeken aanwezig zijn in de winkel. Dit kan namelijk door middel van scannen. Men gaat met een scanner voor de schappen langs en op een beeldscherm komt te staan welke boeken er in het schap staan.

Met al deze voordelen lijkt het logisch dat Selexyz de RFID toepast in haar winkels. Selexyz heeft dan ook besloten om op de RFID tags over te gaan.

Maar er bestaan bezwaren tegen de RFID technologie. Mensen zijn bang dat hun privacy in het geding komt. Er doen verhalen de ronde dat je met een RFID tag in je bezit overal te volgen en te traceren bent. Ook kan er precies gezien worden waar je geweest bent en wat je allemaal gekocht hebt in het verleden. Het lijkt dan ook logisch dat er mensen zijn die tegen deze technologie zijn...

Ook Selexyz weet dat de RFID technologie niet door iedereen geaccepteerd wordt en wil daarom graag te weten komen wát nu precies de bezwaren zijn. Als de bezwaren bekend zijn kan er naar oplossingen gezocht worden om de bezwaren bij de klanten proberen weg te nemen. Daarnaast zal ik ook een samenvatting geven van de voordelen die de RFID technologie voor de consumenten kan hebben. Dit zou Selexyz bijvoorbeeld kunnen gebruiken om haar klanten te overtuigen van het nut van de technologie.

Tot slot is het voor Selexyz handig om te weten komen wat er momenteel in de wetgeving is vastgelegd dat raakvlak heeft met de RFID technologie. Hierbij kan

bijvoorbeeld aan wetgeving vanuit het oogpunt van privacy gedacht worden. Als Selexyz weet wat de wettelijke beperkingen zijn die opgelegd zijn aan het gebruik van de technologie, kan ze hier rekening mee houden. Ze weet dan de randvoorwaarden die door de wet gesteld zijn. Dit zijn samengevat punten die in dit onderzoek aan bod zullen komen. Als deze punten zijn onderzocht zullen er nog enkele aanbevelingen van mij volgen over hoe men, mijns inziens, het best kan communiceren en hoe men de technologie het best in zou kunnen voeren.

## 1.2 De RFID technologie

Voor veel mensen zal het begrip RFID technologie een onbekend begrip zijn. Daarom zal hier eerst een introductie komen over deze technologie.

RFID staat voor Radio Frequency Identification. Het is een techniek die kan identificeren door middel van radiogolven. Hierdoor kan men van een afstand informatie opslaan en lezen van zogenaamde RFID-tags die op of in objecten zitten. RFID-tags zijn RFID chips in combinaties met antennes om zo de gegevens af te lezen.

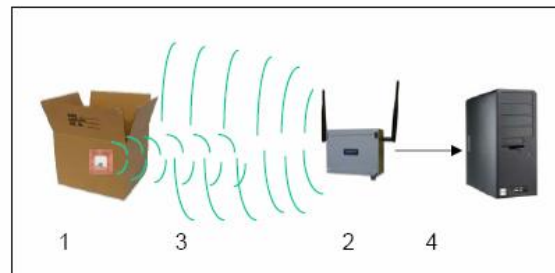
RFID werkt in het algemeen als volgt:

Een chip op een product, 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 eigen radiosignaal op te wekken, waardoor een bericht terug gestuurd wordt aan het leesapparaat. Dit bericht bevat de informatie die opgeslagen ligt in de chip. Het leesapparaat stuurt deze informatie vervolgens door naar achterliggende informatieverwerkende systemen (4) (Min. EZ, 2006).

In de voorbeeldsituatie is uitgegaan van passieve tags. Daarnaast zijn er ook actieve tags die zelf signalen uitzenden door middel van een batterij. Het signaal hoeft dan alleen maar te worden ontvangen. Hier is de mogelijkheid om de tags te volgen groter dan bij passieve tags. Selexyz gebruikt echter alleen maar passieve tags.

Door technologische en prijsontwikkelingen worden de chips steeds kleiner en goedkoper en wordt de technologie steeds vaker toegepast. RFID zal hiermee een bijdrage kunnen leveren aan de economische groei en innovatie.



Afbeelding 2: De werking van de RFID technologie



(Inter)nationaal zijn er hoogspannen verwachtingen over de economische mogelijkheden van de RFID technologie, maar tevens zorgen over de maatschappelijke nadelen ervan.

De RFID chip wordt gezien als de vervanger van de traditionele streepjescode die we nu kennen. Het verschil tussen de twee is dat de streepjescode in het zicht van een scanner moet worden gelezen. Een RFID chip hoeft dit niet. Deze kan op beperkte afstand, door objecten heen en met meerdere tegelijkertijd uitgelezen worden. Voorbeelden van het gebruik hiervan zijn elektronische toegangspasjes in gebouwen, het nieuwe Nederlandse paspoort en de OV-chipcard in het openbaar vervoer (Min. EZ, 2006).

Maar ondanks al de voordelen die hierboven genoemd zijn is de RFID een omstreden technologie. In de Verenigde Staten is er veel ophef geweest toen Wall Mart de RFID technologie toe ging passen op haar producten. Door alle weerstand die er toen is gekomen heeft de introductie van de RFID technologie bij Wal Mart een flinke vertraging opgelopen. Dit heeft Wal Mart dan natuurlijk ook geen goede publiciteit opgeleverd. Net zoals in de Verenigde Staten zijn er ook in Nederland mensen die bezwaren hebben tegen het toepassen van de RFID technologie. Dit bezwaar komt veelal uit het oogpunt van de privacy. Mensen denken dat hun privacy geschaad wordt als ze producten kopen waar RFID tags op zitten. Ze zijn bijvoorbeeld bang dat ze door de tag overal te traceren zijn. Een andere angst onder de mensen is dat bedrijven mensen gaan categoriseren in groepen voor commerciële doeleinden en dat kwaadwillenden gegevens over hen uit kunnen lezen.

## 2. Onderzoeksopzet

### 2.1 Onderzoeksdoel

Om tot een goede onderzoeksopzet te komen moet eerst bekend zijn wat Selexyz wil bereiken met deze opdracht. Daarom zullen nu eerst enkele punten genoemd worden die Selexyz graag te weten wil komen. Selexyz heeft besloten om de RFID technologie in te gaan voeren. Nu wil men graag te weten komen waar men rekening mee moet houden als ze de RFID technologie in een nieuwe winkel in gaat voeren. Er moet een soort 'invoeringsstrategie' komen met punten waar op gelet moet worden en wat men kan doen zodat de RFID technologie zo goed mogelijk gaat lopen. De invoering van de RFID technologie zo voorspoedig mogelijk verlopen. Hierbij zijn verschillende punten te bedenken. Het eerste punt is het volgende:

*-De bezwaren die de klanten van Selexyz kunnen hebben tegen de RFID technologie.*

Het is belangrijk om te weten waar de mensen precies op tegen zijn en wat daar de reden van is. Daarnaast is het de vraag of deze gevaren niet overdreven verhalen zijn door bijvoorbeeld de tegenstanders. Als Selexyz dit te weten komt kan men de bezwaren structureel te lijf gaan en zo voorkomen dat klanten zullen vertrekken bij Selexyz.

Een tweede punt dat men bij Selexyz te weten wil komen is het volgende:

*-De wetgeving die raakvlak heeft met de RFID technologie zoals Selexyz die gebruikt.*

Als Selexyz de RFID technologie invoert is het belangrijk te weten wat er wel en niet toegestaan is. Daarom zal de wetgeving die betrekking heeft met de RFID technologie bekeken worden. Hierbij kun je denken aan restricties via wetten die zijn opgenomen in (inter)nationale wetgeving.

Het derde punt dat van belang is voor Selexyz om te weten is:

*-De voordelen van de RFID technologie die de consumenten zien.*

Deze voordelen zullen onderzocht worden omdat Selexyz hier haar voordeel mee kan doen. Als Selexyz haar klanten kan overtuigen van de voordelen van de RFID technologie zullen ze waarschijnlijk blijven en bestaat er een kans dat er nog meer klanten zullen komen. Communicatie speelt hierin ook een belangrijke rol. De klanten en overige

consumenten moeten namelijk op een bepaalde manier overtuigd worden van de voordelen van de technologie.

Communicatie speelt bij de invoeringsstrategie ook een niet te onderschatten rol. Er kan een goede invoeringsstrategie bedacht worden, maar als deze niet op de juiste manier overgebracht wordt op de klanten is de werking hiervan ook minder. Er is echter geen onderzoeksvraag over de wijze van communicatie. Dit omdat ik een Bestuurskunde student ben en een student in de Communicatiewetenschappen. Ik ben van mening dat ik te weinig expertise heb om dat onderwerp goed genoeg te onderzoeken. Wel zijn er enkele adviezen gegeven aan het eind van het verslag.

Overigens zijn de punten die ik zal onderzoeken niet in het geheel door mijzelf gekozen. De keuze is voor een gedeelte ook door Selexyz gemaakt. Er is mij gevraagd onderzoek te doen naar bezwaren die consumenten tegen de RFID technologie kunnen hebben. Daarnaast is mij gevraagd een onderzoek te doen naar de huidige wetgeving die raakvlak heeft met de RFID technologie zoals Selexyz die gebruikt. Er hoeft ook geen onderzoek gedaan te worden naar welk soort RFID systeem het best gebruikt kan worden. Dit ligt namelijk ook al vast.

Het punt dat over de voordelen gaat is wel door mij zelf geformuleerd. Ik denk dat het bij de voorlichting van klanten van groot belang is dat ze weten wat de voordelen zijn. Klanten willen weten wat 'het ze oplevert' als ze een nieuwe technologie gaan gebruiken.

Samenvattend kan gezegd worden:

*Onderzoeksdoel:*

- Een invoeringsstrategie voor de RFID technologie formuleren.

*Voor de invoeringsstrategie zijn de volgende gegevens nodig:*

- De bezwaren die de klanten van Selexyz kunnen hebben tegen de RFID technologie.
- De wetgeving die raakvlak heeft met de RFID technologie zoals Selexyz die gebruikt.
- De voordelen van de RFID technologie die de consumenten zien.

## *2.2 Onderzoeksvragen*

In dit onderdeel zal ik het hierboven genoemde onderzoeksdoel terug laten komen in de centrale onderzoeksvraag. Het onderzoeksdoel was 'een invoeringsstrategie voor de RFID technologie formuleren'. Hierdoor wordt de centrale onderzoeksvraag als volgt:

*Wat kan Selexyz het beste doen om de invoering van de RFID technologie zo voorspoedig mogelijk te laten verlopen?*

De hierboven geformuleerde handelingsprobleem heb ik samen proberen te vatten in een algemene centrale vraag. Dit is dan ook de vraag:

*Wat zijn de randvoorwaarden bij de invoeringswijze van de RFID technologie bij Selexyz?*

Naar mijn mening is het van groot belang om te kijken wat de invloed van de technologie is bij Selexyz omdat het een commerciële organisatie is. Ze is voor haar bestaan afhankelijk van haar klanten. Het is daarom belangrijk dat ze de opvattingen van haar klanten over de RFID technologie te weten komt. Op deze manier kan ze rekening houden met de opvattingen van de klanten tijdens de invoering van de RFID technologie. Zo kan men er alles aan doen deze soepel te laten verlopen. Als er klanten zijn die vinden dat er nadelen zijn verbonden aan de technologie dan kunnen die bijvoorbeeld voorgelicht worden. Het is daarom ook handig om te weten hoe precies gecommuniceerd kan gaan worden met klanten. Moeten de medewerkers veel over de technologie weten en de klanten voorlichten of moeten er flyers in de winkels komen te liggen?

Naast de centrale onderzoeksvraag zijn er nog enkele deelvragen opgesteld die helpen de centrale vraag te beantwoorden. Deze drie onderzoeksvragen zijn ook in het onderzoeksdoel genoemd en zijn als volgt:

- Wat zijn de voordelen die de consumenten zien als Selexyz de RFID technologie invoert?
- Wat kunnen de bezwaren van de klanten zijn als Selexyz de RFID technologie invoert?
- Wat zijn de wettelijke restricties bij de RFID technologie zoals gehanteerd door Selexyz?

De eerste onderzoeksvraag gaat over de voordelen die de consumenten zien als Selexyz de RFID technologie op grotere schaal zal invoeren. Er zal onderzocht worden welke voordelen de consumenten zien als Selexyz in meerdere winkels van een gewone boekwinkel omschakelt naar een winkel met de RFID technologie. Als Selexyz er voor kiest om haar klanten voor te lichten over de technologie is het van belang om te weten wat het de klanten nu precies voor voordeel oplevert. Door op voordelen te wijzen zullen klanten de RFID technologie misschien wel sneller gaan accepteren.

In de tweede onderzoeksvraag zullen de bezwaren van de klanten bij de RFID technologie onderzocht worden. Er wordt bestudeerd wat de bezwaren van klanten zijn als een Selexyz-winkel de RFID technologie toepast. Het is zoals al eerder gezegd handig om te weten wat de bezwaren precies zijn omdat klanten anders misschien weg zullen blijven.

De derde onderzoeksvraag gaat over de beperkingen die de wet Selexyz oplegt. Er zal gekeken worden naar de huidige wetgeving die er bestaat op het gebied van de RFID technologie. Als deze duidelijk in beeld is kan er gekeken worden wat de beperkingen zijn voor Selexyz. Ze wil natuurlijk niet (onbewust) de wetgeving overtreden. Als we de restricties weten kan Selexyz ook kijken wat de eventuele mogelijkheden zijn.

### *2.3 Plan van aanpak*

Nu is het tijd om aan te geven hoe de gedefinieerde onderzoeksvragen geoperationaliseerd gaan worden.

De eerste deelvraag die geformuleerd is ging over de voordelen die de consumenten zien als Selexyz de RFID technologie toe zal passen. Als eerste zal ik hier gebruik gaan maken van reeds verrichte onderzoeken. Er bestaan namelijk al enkele onderzoeken waarbij aan de consument zélf is gevraagd wat zij als grootste voordelen en grootste nadelen van de RFID technologie vinden. Het is zaak om die onderzoeken te vinden en hier bruikbare gegevens uit te halen. Daarnaast zal ik gebruik gaan maken van een zogenaamde expert opinion. Dit is de mening en kennis van iemand die, in dit geval, veel verstand van het onderwerp RFID heeft. Ik zal tijdens mijn onderzoek met diverse mensen bij Selexyz spreken die hier verstand van hebben. Zij kunnen wellicht voorzien wat de voordelen van de invoering van de RFID technologie voor de consumenten zijn. Om een tunnelvisie te voorkomen heb ik ook een expert van buiten Selexyz geraadpleegd. Dit was Mary Brown, een expert in RFID veiligheid en faculteitslid en docent informatietechnologie aan de Capella University in Minneapolis. Meer mensen heb ik, onder andere door de korte tijd van het onderzoek, niet kunnen interviewen.

In deze onderzoeksvraag zal er ook een kleine enquête gehouden worden naar de belangrijkheid van de voordelen van de RFID technologie.

Als laatste zal er een literatuurstudie verricht worden. In verschillende theorieën is te lezen hoe mensen reageren op de invoering van nieuwe technieken. Ook zal er een zoektocht plaatsvinden naar bestaande literatuur over de voordelen van de RFID technologie. Door mijn begeleiders van de Universiteit Twente ben ik van tevoren al op een theorieën gewezen die van waarde kan zijn. Dit is de theorie van Everett Rogers over early and late adapters uit 1962.

De tweede deelvraag die onderzocht zal gaan worden gaat over de bezwaren die de klanten tegen de invoering van de RFID technologie hebben. Hierbij ben ik van plan een vergelijkbare manier van onderzoek te doen als bij deelvraag 1. Hier zal namelijk ook gezocht worden naar eerdere onderzoeken die hebben plaats gevonden. Het zelf uitvoeren van onderzoeken of het afnemen van enquêtes gaat niet lukken in de relatief korte tijd die voor deze opdracht staat. Vooral ook omdat er voor een representatief

onderzoek een groot aantal mensen ondervraagd moet worden vind ik. Ook bij deze deelvraag zal ik vragen stellen aan de experts van Selexyz over de bezwaren die de klanten kunnen hebben. Daarnaast zal ik ze ook naar de eigen mening over deze deelvraag vragen. Tot slot zal ik gebruik maken van een literatuurstudie. Een voorbeeld hiervan is de theorie van Peter Morville over de Ambient findability uit 2005.

De derde deelvraag die ik zal gaan behandelen is een andere qua opzet. Ze gaat namelijk over de wettelijke restricties van de RFID technologie. Hierbij zal er gebruik gemaakt worden van eerdere onderzoeken die verricht zijn naar de wettelijke restricties bij de RFID technologie. Een van de onderzoeken is in 2006 verricht door het Ministerie van Economische Zaken. Daarnaast zal er 'logischerwijs' gebruik gemaakt worden van de wetbundel. Ik zal echter geen gebruik maken van de expert opinion. Er zijn namelijk al eerdere onderzoeken verricht naar de wettelijke restricties door experts. Hier maak ik dan ook gebruik van. Op grond van de literatuur heb ik het idee dat er niet veel meer te behalen valt. Ook als gevolg van de beperkte tijd heb ik de keuze moeten maken om geen experts te interviewen. Op grond van de informatie die ik al had leek me dit een legitieme keuze.

### 3. Wat zijn de voordelen die de consumenten zien als Selexyz de RFID technologie invoert?

In deze deelvraag zal gekeken worden wat de voordelen van de RFID technologie precies zijn volgens de consumenten. Als de klanten van Selexyz weten wat de voordelen voor hen kunnen zijn zullen ze waarschijnlijk minder bezwaren hebben tegen de technologie. De verschillende voordelen van de RFID technologie heb ik als volgt samengesteld: De *dalende prijzen* en de *aankoopsgesties op basis van eerdere aankopen* zijn afkomstig uit een onderzoek van R&M Interactive. Er wordt elk half jaar door R&M Interactive een zogeheten Emerce RFID Monitor uitgevoerd. Dit is een onderzoek onder 1073 Nederlanders. Hierin kunnen ze aangeven hoe ze over de RFID technologie denken. In het eerste halfjaar van 2004 werden er een aantal denkbare toepassingen van de RFID technologie aan de respondenten voorgelegd.

Het terugvinden van gestolen goederen stond daar op nummer één maar is niet opgenomen in de voordelen omdat dit niet van toepassing is op Selexyz. Bij afrekening wordt de tag vernietigd en zijn de producten waar de tag op zit niet meer te traceren.

*Nederlanders zien veel voordelen van RFID bij het terugvinden van gestolen goederen (78% van de respondenten) en dalende prijzen als gevolg van lagere kosten in de logistieke keten (63%). Aankoopsgesties op basis van eerdere aankopen ziet slechts 10% als een mogelijk voordeel (www.rfid.emerce.nl).*

Het voordeel *kortere wachttijden bij de kassa* is afkomstig van een expert opinion. Ik heb eenmaal contact gehad met Mary Brown. Zij is een expert in RFID veiligheid en een faculteitslid en docent informatietechnologie aan de Capella University in Minneapolis, Minnesota. Op het internet kwam ik een artikel van haar tegen en heb zodoende contact met haar opgenomen om te vragen of ze nog suggesties had voor me. Zij was van mening dat het afrekenen sneller gaat als producten op afstand al gelezen kunnen worden. Daar komt bij dat er bij de kassa ook minder boeken besteld zullen worden omdat nu elders in de winkel kan.

Het voordeel van *snel en gemakkelijk bestellen van boeken* is bij me opgekomen na de rondleiding die ik van Jan Veninga heb gekregen in Almere. Hij wees me op het gemak en de snelheid van het bestellen van boeken via de RFID technologie in combinatie met het Klant Informatie Punt. Daarnaast was dit voordeel ook terug te vinden in de Powerpoint presentaties die Jan Vink mij toegestuurd heeft.

Het laatste voordeel de *persoonlijke reclame* heb ik niet via een bron gekregen maar is zelf bij me opgekomen. Na het lezen van enkele forums die over de RFID technologie gingen viel me op dat toch veel mensen voordelen zien in de RFID technologie.

### 3.1 Voordelen die de consumenten zien

Een eerste voordeel dat genoemd kan worden zijn de *kortere wachttijden bij de kassa*. In ons geval de kassa's van Selexyz. Bij de RFID technologie wordt er een chip op de boeken geplaatst die bij de kassa meteen uitgelezen wordt. Wat dit betreft is er weinig voordeel ten opzichte van de streepjescode. Maar als iemand meerdere boeken heeft kunnen die tegelijk uitgelezen worden. Dit scheelt wel in de afrekening. Door technologische ontwikkelingen is het denkbaar dat er in de toekomst helemaal geen kassa's meer nodig zijn. Mensen kunnen dan met boeken naar buiten lopen en bij het verlaten van de winkel wordt gecontroleerd met hoeveel en welke boeken de klant weggaat. Het bedrag kan vervolgens automatisch via de bankrekening afgeschreven worden. Dit scheelt veel meer in de afrekening want die is er namelijk niet meer.

Hierdoor kan het afrekenen dus tot enkele minuten sneller gaan.

Daarnaast is het ook denkbaar dat de *prijzen voor de klant dalen*. De boekenprijs staat dan wel vast in de wet, maar als je bepaalde kosten kunt drukken heb je een lagere prijs nodig om dezelfde winst te behalen. De prijzen voor de klanten dalen door verschillende redenen. Ten eerste daalt de prijs als gevolg van lagere kosten in de logistieke keten. Alle boeken die van het Centraal Boekhuis komen zijn immers van een tag voorzien. Bij Selexyz gaan ze alleen door een tunnel en er is duidelijk wat er allemaal binnen is gekomen. Dit scheelt veel tijd met het controleren van boeken en eventuele foute bestellingen zijn snel te ontdekken door de dozen bij binnenkomst te scannen. Naast dalende kosten door lagere kosten in de logistieke keten kunnen de prijzen ook dalen door het verdwijnen van kassa's. Als de afrekening minder wordt kan er misschien een aantal verdwijnen. Dit scheelt in personeelskosten. Het is ook denkbaar dat alle kassa's verdwijnen als er afgerekend kan worden door gewoon door poortjes te lopen bij het naar buiten gaan. De producten worden dus minder duur en dit is een groot voordeel voor de klant. Voor precieze gegevens over prijsdalingen heb ik echter geen gegevens gevonden.

Een derde voordeel is dat klanten *aankoopsgesties kunnen krijgen op basis van eerdere aankopen*. Dit kan gebeuren door middel van de SmartCard en het Klant Informatie Punt (KIP). Een SmartCard is een toepassing waarbij een chipcard wordt uitgerust met RFID technologie. Hierdoor wordt contactloze communicatie mogelijk. Dit in tegenstelling tot de magneetstrip op de huidige bankpassen waarbij fysiek contact moet worden



Afbeelding 3: Een Klant Informatie Punt



gelegd. Een contactloze smartcard bevat een kleine microprocessor met een beperkt geheugen en een kleine rekeneenheid net als in de huidige bankpassen. Hierop kunnen gegevens worden opgeslagen zoals het koopgedrag van de klant (Min EZ, 2006).

Als een klant vaak boeken koopt die over geschiedenis gaan wordt dit door de SmartCard genoteerd. Als de klant vervolgens bij de KIP komt kan hij een aankoopadvies krijgen over bijvoorbeeld de nieuwste boeken die bij zijn eerdere aankopen passen. Geschiedenis in dit geval.

Een ander voordeel dat daar op lijkt is het *verkrijgen van persoonlijke reclame*. Iedereen kent de algemene reclamefolders die men dagelijks in de bus krijgt. De helft wordt vaak niet eens gelezen. Een voordeel van persoonlijke reclame is dat het reclame betreft over onderwerpen die je aanspreken. Deze persoonlijke reclame wordt verzorgd op basis van je eerdere aankopen. Deze gegevens worden bewaard en zo is het mogelijk een samenstelling van reclame te maken die jou aanspreekt.

Het laatste voordeel is dat de KIP daarnaast helpt met het *zoeken en bestellen van boeken*. Als een boek niet aanwezig is dan kan deze snel en simpel besteld worden via de KIP of via het internet. Als je op zoek bent naar een specifiek boek dat er niet is kun het bestellen via de KIP of het internet. Als het boek vervolgens besteld is kan de klant een email of sms krijgen als hij hier voor gekozen heeft. Daar komt bij dat eventuele foute bestellingen sneller ontdekt worden als de boeken binnen komen. Er wordt meteen gescand welke boeken er in de dozen zitten en een eventuele foute bestelling wordt er meteen uit gepikt. De keuze om van de SmartCard en de KIP gebruik te maken is vrijwillig. Daarnaast blijven er namelijk nog altijd medewerkers in de winkel voor bijvoorbeeld de kassa's en bevoorrading. Deze kunnen de klanten dan nog helpen. Mochten er mensen zijn die geen gebruik willen maken van de KIP dan kunnen ze nog op de 'oude manier' geholpen worden.

Als hier sprake van is zien we een verschil tussen mensen die snel geholpen willen worden graag gebruik maken van de nieuwe technologie, en mensen die liever traditioneel geholpen worden en niet veel van de nieuwe technologieën moeten hebben. Dit verschijnsel zien we terug in de theorie van diffusion of innovations van Rogers uit 1962. Deze theorie gaat onder andere over de early and late adapters. Als er een nieuwe technologie komt zijn er 5 stadia te beschrijven waar de klanten doorheen gaan. Dit heet de Innovation Decision Theory (Rogers, 1995).

Klanten moeten eerst kennis nemen van de innovatie (kennis), ten tweede moeten ze overtuigd raken van de waarde van de innovatie (overtuiging). ten derde moeten ze besluiten de innovatie aan te nemen (beslissing), ten vierde moet de innovatie worden geïmplementeerd (implementatie), tot slot moet de beslissing worden herbevestigd of afgewezen (confirmatie).

Hieruit komen early en late adapters voort. Early adapters zijn mensen die nieuwe technologieën snel oppikken en gebruiken. Late adapters zijn huiveriger en zullen de nieuwe technologie niet meteen gaan gebruiken.

Een voorbeeld ter illustratie. Een student wil graag snel het boek hebben dat hij nodig heeft en gaat daarna meteen weer weg. Daarnaast zijn studenten jong en zullen ze nieuwe technologieën waarschijnlijk sneller accepteren. Een student zou in dit voorbeeld een early adapter zijn. Een bejaarde man daarentegen gaat in de boekwinkel op zoek naar een mooi boek en wil daarbij graag geholpen worden door een medewerker. De bejaarde man zal niet met behulp van een nieuwe technologie willen zoeken. In dit geval is er sprake van een late adapter (Rogers, 1995).

### *3.2 Voordelen rangschikken op belangrijkheid*

Om de verschillende voordelen te rangschikken op belangrijkheid zal ik nu gebruik gaan maken van een keuzetechniek van Thomas Saaty. De techniek is het Analytic Hierarchy Process (AHP). De AHP maakt gebruik van gepaarde vergelijkingen om oordelen te kunnen vellen over welke variabele zwaarder weegt in het keuzeprocess. Zo komt er een rangschikking op grond van belangrijkheid (Saaty, 1990).

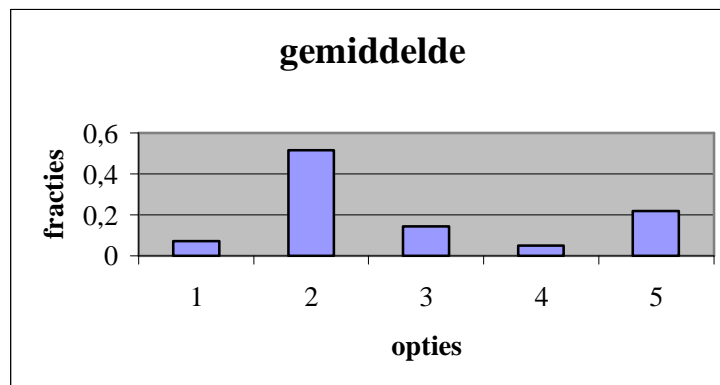
De verschillende voordelen die de RFID technologie heeft zullen paarsgewijs vergeleken worden en er zal door verschillende respondenten een rangschikking gemaakt worden. Deze AHP is echter een pilot door mijzelf uitgevoerd onder een klein aantal respondenten. Ik heb hen een lijst met paarsgewijze vergelijkingen voorgelegd en zo konden de respondenten aangeven welke voordelen zij het belangrijkste vonden. Hierbij ben ik mij bewust van de validiteitsbeperkingen die er zijn. Als ik mensen in een boekwinkel had gevraagd, of zelfs als ik dezelfde respondenten in de paarsgewijze vergelijkingen in een boekwinkel had voorgelegd, zouden ze misschien wel anders kiezen. Het kan voor Selexyz verstandig zijn om zelf eens de AHP methode uit te voeren onder haar klanten. Op deze manier komt ze te weten wat de klanten belangrijke voordelen vinden. Dit kan natuurlijk ook in samenwerking met Universiteit Twente gebeuren.

Hieronder staat de AHP methode die ik toegepast heb in stappen uitgelegd.

1. Als eerste krijgen alle voordelen een aanduiding. Schematisch gezien ziet dit er als volgt uit:

Voordeel	Aanduiding
Kortere wachttijden bij de kassa	C1
Lagere prijs van de boeken	C2
Aankoopsgesties o.b.v. eerdere aankopen	C3
Persoonlijke reclame	C4
Snel en makkelijke bestellen en vinden van boeken	C5

2. Daarna wordt er een schaal opgesteld met verschillende keuzemogelijkheden. Bij de AHP methode wordt gebruik gemaakt van een schaal met 9 keuzemogelijkheden. Te weten:
  - Heel veel belangrijker
  - Veel belangrijker
  - Belangrijker
  - Iets belangrijker
  - Neutraal
  - Iets minder belangrijk
  - Minder belangrijk
  - Veel minder belangrijk
  - Heel veel minder belangrijk (Saaty,1990)
3. Vervolgens zullen C1, C2, C3, C4 en C5 paarsgewijs met elkaar vergelijken. Zo worden C1 met C2, C2 met C3, C3 met C1 et cetera vergeleken.
4. De respondenten kunnen bij elk van de paarsgewijze vergelijkingen een van de 9 keuzemogelijkheden kiezen. Vb. respondent 1 vindt C1 veel belangrijker dan C2. Op deze manier wordt er een rangschikking gemaakt. Zo wordt ook bekend welke voordelen het zwaarst wegen en welke minder zwaar.
5. Vervolgens worden de uitkomsten schematisch weergegeven in histogrammen. De som van alle histogrammes volgt hieronder. De histogrammen per respondent zijn in de bijlage te vinden.



*Afbeelding 4: De verschillende voordelen weergegeven volgens de AHP methode in een histogram*

Bij de output zijn verschillende gewichtsscores te zien in het histogram. De score is samengesteld op grond van paarsgewijze vergelijkingen van verschillende variabelen. Per variabele wordt aangegeven hoeveel het percentage belang is dat aan een desbetreffende variabele kan worden toegekend. De helft van de fracties (51,5%) gaat uit naar variabele 2. Deze heeft dus het zwaarste gewicht. Op ruime afstand volgt variabele 5 met iets meer dan 22%. Variabele 3 volgt op de derde plaats met ongeveer

14,3%. Veruit de minste stemmen gingen uit naar variabelen 1 en 4 met respectievelijk 7,2% en 4,8%.

### *3.3 Conclusie*

We zien dat de lagere prijzen van de boeken het belangrijkste voordeel is voor de consumenten die aan deze enquête hebben meegedaan. Meer dan de helft vindt dit voordeel het belangrijkste. Het lijkt dus zaak dat Selexyz de dalende prijzen (in de logistieke keten) benadrukt in haar campagne voor de RFID technologie. Het sneller en makkelijker bestellen van boeken is op de tweede plaats geëindigd op grond van belangrjkheid. Dit voordeel eindigde op iets meer dan 22%. Ook aan dit voordeel zou Selexyz kunnen denken als ze voorlichting geeft over de voordelen van de RFID technologie. De derde plaats in de volgorde van belangrjkheid is voor de aankoopsgesties op basis van eerdere aankopen. Deze kreeg 14,3% van de stemmen. De kortere wachttijden (7,2%) en persoonlijke reclame (4,8%) eindigden achteraan. Dit zijn voordelen die niet als erg belangrijk werden beschouwd in deze enquête. Als Selexyz de consumenten op voordelen zou wijzen weet men dat, in dit onderzoek, de voordelen kortere wachttijden bij de kassa en persoonlijke reclame niet als erg belangrijk worden gezien.

#### 4. Wat kunnen de bezwaren van de klanten tegen de RFID technologie zijn?

Ter introductie op de tweede deelvraag zal er eerst een case uit de VS komen. De VS lopen op ons voor wat betreft de RFID technologie, en hier kunnen we dus enkele praktische zaken van afkijken. Uit de case blijkt dat niet zomaar alles geaccepteerd wordt door de consumenten. Er kan door Selexyz een les getrokken worden door te kijken wat destijds de grootste bezwaren van de consumenten waren. Hier kan Selexyz vervolgens rekening mee houden met haar invoeringsstrategie voor de RFID technologie.

In hoofdstuk 4.2 zal er gekeken worden naar wat de grootste bezwaren van de Nederlandse consument zijn.

##### 4.1 Case Wal-Mart

Het supermarktconcern Wal-Mart dat vooral gevestigd is in de Verenigde Staten is één van de pioniers op het gebied van de toepassing van de RFID technologie. In 2005 heeft Wal-Mart zijn honderd grootste toeleveranciers verplicht al hun pallets en dozen van RFID-chips te voorzien.

Wal-Mart voorziet voordelen in het gebruik van de RFID technologie. Behalve sneller afrekenen bij de kassa heeft dat nog wat aanvullende voordelen, zoals het eenvoudiger maken van anti-diefstalcontroles en het registreren van klantaankopen. Door het gebruik van RFID kun je supersnel de inhoud van je winkelwagen laten scannen en laten afrekenen. RFID gekoppeld aan je eigen "bonuskaart" met RFID. De kassa ziet precies wie je bent. Wat je koopt. En hoeveel korting je krijgt omdat je bijvoorbeeld een trouwe koper bent van een bepaald merk melk. Wat technisch nog niet gebeurt is dat er ook afgerekend kan worden via RFID.

Maar op het registreren van de klantgegevens is in de Verenigde Staten veel kritiek gekomen. In de Verenigde Staten is het privacygegeven dan ook het grootste bezwaar tegen de toepassing van de RFID technologie. Met RFID kun je product- en aankoopgegevens één op één aan persoonsgegevens koppelen. Een hemel voor marketingmensen, maar niet iets waar privacyorganisaties warm voor lopen.

'Als de techniek ver genoeg is kunnen winkeliers profielen van hun klanten aanleggen', waarschuwt de Amerikaanse actiegroep Consumers Against Supermarket Privacy Invasion and Numbering (Caspian).

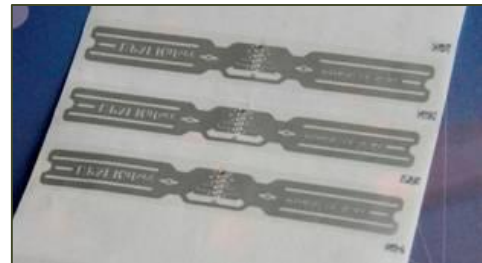
Caspian verworf veel beroemdheid toen ze ontdekten dat Wal-Mart onaangekondigd proeven nam met RFID op scheermesjes. Die dienden niet om het voorraadbeheer te automatiseren, maar om diefstal tegen te gaan. Als een klant meer dan twee pakjes pakt, slaat het schap alarm ([www.zibb.nl](http://www.zibb.nl)).

Door deze ontdekking zakte het vertrouwen van de Amerikaanse consument in de RFID technologie nog verder. Uit dit Amerikaanse voorbeeld blijkt dat het verstandig is om openheid te geven over het toepassen van de RFID technologie.

Selexyz heeft het voordeel dat het Centraal Boekhuis (CB), waar ze haar boeken bestelt, de RFID technologie ook al wordt toegepast. Ze hoeft hier met het CB geen onderhandelingen meer over te voeren.

#### 4.2 Bezwaren RFID in Nederland

In Nederland is momenteel zo'n twaalf procent van de bevolking bekend met de term RFID. (Capgemini 2005a) Ongeveer de helft van de Nederlandse consumenten die bekend zijn met RFID ziet voornamelijk voordelen, slechts zeven procent daarvan ziet voornamelijk nadelen, de resterende consumenten zien geen grote voor of nadelen of hebben geen mening.



Afbeelding 5: Stickervel met 3 RFID tags

Men maakt zich in Nederland dus ook zorgen over RFID. Hierbij worden als belangrijkste issues genoemd: het gebruik van (persoons)gegevens door derden, het kunnen volgen van consumenten via hun aankopen, het lezen van tags over langere afstand, en de toename van direct marketing. Al deze zorgen zijn gerelateerd aan privacy; de consument maakt zich minder zorgen over gezondheidskwesties (zoals straling) en milieuproblemen (Capgemini 2005a).

Daarnaast geeft zo'n zeventig procent van de consumenten aan dat zij eerder RFID-getagde producten zouden kopen als er wettelijke privacybescherming zou zijn voor RFID (Capgemini 2005a). Hoe de resultaten uit dit onderzoek zich tot feitelijk gedrag verhouden is niet bekend.

Zoals we hierboven zien voorzien de meeste Nederlanders vooral voordelen in het gebruik van de RFID technologie. Over de voornaamste nadelen die de Nederlanders zien zullen we het in deze deelvraag gaan hebben.



Afbeelding 6: Traditionele streepjescode

In tegenstelling tot streepjescodes kunnen RFID tags op afstand worden uitgelezen zonder dat de consument dit door heeft.

Hier ligt dan ook een mogelijk bezwaarpunt van de klant. Er is een groep mensen die niet wil dat er steeds meer informatie over hen bekend wordt en opgeslagen wordt.

Daarnaast is het is voor een consument niet altijd duidelijk of een product een RFID-tag bevat. Nu de RFID tags steeds kleiner worden kunnen ze nog makkelijker worden verwerkt in producten of op de verpakking van producten zonder dat consumenten dat door kunnen hebben. Hierdoor kan het voor de mensen onduidelijk zijn of ze RFID-tags bij zich dragen en zo ja of de informatie op deze RFID-tags informatie over hen overdraagt aan onbekende personen of instanties (Min EZ, 2006). Het is goed mogelijk dat er mensen zijn die met een tag-reader ongevraagd andere tags kunnen lezen en zo informatie kunnen inzien die niet voor hen bestemd is.

Dit verschijnsel wordt ook wel Ambient Findability genoemd. Dit betekent dat er een wereld ontstaat waarin er steeds meer gegevens over mensen opgeslagen worden en dat er daardoor steeds meer gegevens bekend zijn over iedereen en dat die overal en altijd gelezen kunnen worden (Morville, 2005). Bij ambient findability zal er een vergrote kans zijn op privacyrisico's.

In de publicatie van het ministerie van Economische Zaken genaamd Notitie 'RFID in Nederland' uit 2006 worden de drie grootste privacyrisico's genoemd.

Het eerste privacyrisico is het volgen van mensen. Het volgen van mensen is mogelijk doordat RFID-tags het mogelijk maken om een individueel product te volgen. Hiermee is het ook mogelijk om een specifiek persoon te volgen. Wanneer een consument een product bij zich draagt waarvan de RFID-tag kan worden uitgelezen ontstaat er een privacyrisico. Op dat moment kan deze persoon namelijk in theorie gevolgd worden aan de hand van het artikel dat hij of zij bij zich draagt (Min EZ, 2006).

Het tweede privacyrisico is het categoriseren van mensen. Met RFID-systemen is het mogelijk om grote hoeveelheden informatie te verzamelen. Deze informatie kan gebruikt worden om bepaalde kenmerken van een individu in kaart te brengen. Hiervoor moet de verzamelde informatie op de RFID tags gekoppeld worden aan persoonsgegevens. Met een dergelijk profiel kan er vervolgens een beter inzicht komen in het gedrag van individuele personen. Deze informatie kan bijvoorbeeld worden gebruikt om onderscheid te maken tussen verschillende categorieën consumenten (Min EZ, 2006).

Het categoriseren van mensen is bij de marketing van producten overigens een gebruikelijke en bekende methode en ook algemeen aanvaard, mits dit op een deugdelijke grondslag gebeurt. Soms is daar expliciet toestemming voor nodig van de betrokken personen. Bij RFID-technologie is het voor de consument niet duidelijk wie de informatie kan lezen en wat daar vervolgens mee gebeurt.

Tot slot is er het derde privacyrisico, het uitlezen van persoonsinformatie. Dit laatste risico gaat over de mogelijkheid om met bijvoorbeeld een draagbare reader op afstand in huizen of boodschappentassen van mensen te "kijken". Dit draagt een risico met zich

mee omdat kwaadwillenden op deze manier doelgericht kunnen gaan beroven of inbreken aan de hand van de verzamelde informatie (Min EZ, 2006).

#### *4.3 Relativeringen bij de privacyrisico's*

Overigens zijn er ook relativeringen te bedenken bij elk van de, door het Ministerie van EZ genoemde, privacyrisico's.

Het 'track en trace' idee, dat overal uitgelezen kan worden waar je bent en waar je geweest bent, waar veel mensen bang voor zijn gaat niet op. En wel om twee verschillende redenen. Ten eerste is er namelijk een elektromagnetisch veld van readers nodig om de passieve tags, die Selexyz gebruikt, uit te lezen. Het bereik van zo'n reader is maximaal 10 meter. Alleen als de tag in een veld is kan gezien worden dat de tag echt bestaat. Als iemand in zo'n dergelijk veld komt kan het 'getracked' worden. Immers in het veld kan dan gezien worden waar je bent. Maar als je het veld van maximaal 10 meter verlaat valt niet meer van de readers af te lezen waar je bent. Voor een continue tracement moet er een elektromagnetisch veld van vele miljoenen readers zijn in een grote dichtheid. Zelfs in een winkel is dit economisch niet verantwoord (Hardgrave en Miller, 2006). Als een dergelijk netwerk in de toekomst wel zou ontstaan, moet nog aan een tweede voorwaarde worden voldaan. De tweede voorwaarde is dat diegene die iemand wil volgen ook toegang heeft tot de systemen en de achterliggende databases. De RFID-tag zendt namelijk geen persoonsgegevens uit maar slechts een unieke code. Een eventuele koppeling met persoonsgegevens kan alleen door koppeling van verschillende systemen en bestanden tot stand worden gebracht. Het is niet te verwachten dat één persoon of organisatie toegang zal hebben of zelfs kunnen krijgen tot allerlei losse systemen die in bezit en beheer zijn bij andere organisaties. Als we naar al deze argumenten kijken zal het volgen van mensen dus niet snel gebeuren.

Ook bij het categoriseren van mensen zijn relativeringen te plaatsen. Het categoriseren van mensen kan worden samengevat als op basis van verzamelde gegevens een profiel van een persoon aanmaken. Om voor commerciële organisaties een interessant profiel op te stellen moet er meer informatie beschikbaar zijn dan alleen een uniek nummer van een product dat een persoon bij zich draagt. Men moet dan ook over de persoonsgegevens beschikken. Alleen de eigenaar van de database is daartoe in staat. Overigens is de angst dat bedrijven een profiel van hun klanten maken niet nieuw. Met de komst van digitale kassa's, klantenkaarten en elektronisch betalen bestaat deze mogelijkheid al geruime tijd. De komst van RFID betekent alleen dat er (nog) meer data beschikbaar komen. Op deze data zijn dezelfde privacy-regels van toepassing als op de klantenkaarten en dergelijke.



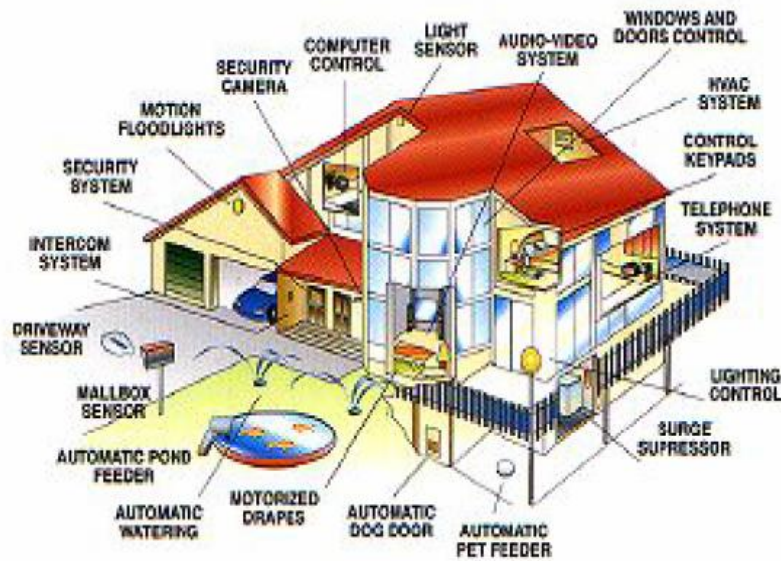
Tot slot het uitlezen van de persoonsinformatie. Het op afstand lezen welke goederen een persoon in huis heeft of bij zich draagt wordt pas actueel als de RFID-technologie op grote schaal wordt gebruikt. Momenteel bevatten maar weinig producten een RFID-tag. Op de tags staan bovendien geen persoonsgegevens. Wil een kwaadwillend iemand deze gegevens weten dan moet men in een andere database zijn. Bijvoorbeeld de database van de verkoper van het product. Als deze database voldoende is beveiligd levert het uitlezen van een RFID-tag dus geen informatie op over het product waar de tag aan is bevestigd (Min EZ, 2006). Beveiligen kan door middel van codes, wachtwoorden en een beperkt aantal medewerkers dat toegang heeft tot de database. Daarnaast is het ook niet mogelijk om tags in huizen uit te lezen vanaf de straat om zo te kijken wat er in huis is. Ten eerste is een passieve tag maar vanaf maximaal 10 meter af te lezen. Iemand die de gegevens wil uitlezen moet dus wel enorm dicht bij het huis komen. Ten tweede valt het ook niet mee om de tags uit te lezen omdat het signaal van een RFID-tag verstoord wordt door water en metaal. Het is dus maar de vraag of er überhaupt nog iets uit te lezen valt (Hardgrave en Miller, 2006). Het verhaal dat er tags die in huizen zijn uitgelezen kunnen worden gaat niet op.

#### *4.4 Conclusie*

Men kan zich ook voorstellen dat er consumenten zijn die het niet erg vinden om iets van hun privacy in te leveren ten behoeve van het gebruiksgemak. De RFID technologie brengt zoals we gelezen hebben ook voordelen met zich mee.

De angst en tegenstand tegen een nieuwe technologie komt namelijk ook voort uit angst voor iets onbekends. Mensen weten niet wat RFID precies inhoudt en dit bied tegenstanders de mogelijkheid om reclame tégen een nieuwe technologie te maken. Een voorbeeld hiervan is het gebruik van de mobiele telefoon. Hier waren eerst ook veel mensen op tegen omdat je met een mobiele telefoon overal te traceren bent. Het verhaal van Ambient Findability gaan voor de mobiele teltefoon, de RFID tags en voor een hoop andere technologiën op. Dit is in de bovenstaande afbeelding te zien. Er komen steeds meer technologiën die 'verraden' waar je bent. Met een mobiele telefoon is het zo dat je altijd en overal te traceren bent. Hier is bij de RFID technologie geen sprake van als de tag passief is of als de tag onklaar is gemaakt. Wat dat betreft is er dus niets nieuws onder de zon wat de privacy betreft.

Voor nu veranderd er niet zo heel veel met de invoering van de RFID technologie. De techniek die gebruikt wordt is alleen nieuw. Het volgen van mensen is niet mogelijk doordat de tag onklaar wordt gemaakt. Het opslaan van klantgegevens kan zonder de RFID technologie ook plaatsvinden. Ik



*Afbeelding 7: Steeds meer technologie in en om het huis*

vermoed zelf dat de grootste angst de mogelijkheden van de RFID technologie in de toekomst zijn. De mogelijkheden zijn enorm en ik denk dat het onbekende de mensen bang maakt.

Dit is in het verleden ook gebeurd. Er werd door de tegenstanders van mobiele telefoons ook ingespeeld op de 'gevaren' van de mobiele telefoon. Tegenwoordig heeft bijna iedereen een mobiele telefoon en horen we dit bezwaar bijna niet meer. We hebben het meer over de voordelen dan over de nadelen die de mobiele telefoon heeft. De voordelen wegen bij de mobiele telefoon op tegen de nadelen. Dit betekent misschien wel dat een nieuwe technologie eerst een bepaalde 'acceptatieperiode' heeft. Mensen hebben een bepaalde tijd nodig waarin ze technologie gebruiken en zich bewust worden van het feit dat er voordelen aanzitten waar ze echt iets aan hebben. Op deze manier zullen ze ook minder over de nadelen beginnen. Hier past de theorie van Rogers (1962) bij. Hij stelt dat mensen een nieuwe technologie sneller accepteren naarmate ze zich meer bewust worden van de voordelen die eraan zitten. Hoe meer voordelen, hoe sneller mensen de nadelen lijken te vergeten. Het is niet ondenkbaar dat dit bij de RFID technologie ook zo zal zijn. De RFID technologie brengt dermate veel gemak met zich mee dat mensen bereid zijn wat privacy in te leveren. Mensen moeten zich eerst bewust worden van de voordelen die er aan de RFID technologie zitten. Vervolgens zullen ze de 'nadelen' voor lief nemen. En misschien zijn er wel helemaal geen risico's aan verbonden. Dit is iets dat niet te plannen valt, dit zal de toekomst voor een groot gedeelte uit moeten wijzen.

## 5. Wat zijn de wettelijke restricties bij de RFID technologie zoals gehanteerd door Selexyz?

In dit hoofdstuk zullen we onderzoeken wat de door de wet gestelde voorwaarden zijn waar Selexyz aan moet voldoen als ze de RFID technologie in meerdere winkels in gebruik wil nemen. Voor Selexyz is het bekijken naar de wettelijke aspecten de eerste stap op weg naar een goede introductie van de RFID technologie. Deze mogen natuurlijk niet overtreden worden en daarom wordt bij deze deelvraag gekeken naar de beperkingen die opgelegd worden door de wet.

Bij de selectie van de wetten heb ik eerst gebruik willen maken van de expert opinion. De desbetreffende docent aan de Universiteit wilde zijn medewerking echter niet verlenen aan de opdracht. Zodoende heb ik gebruik gemaakt van de literatuur van de heer Holvast. Hij bezit een advies- en onderzoeksbureau op het gebied van privacybescherming. Het bureau legt de nadruk op de Wet Bescherming Persoonsgegevens en de internationale richtlijnen van de EU waar Nederland zich aan moet aanpassen. Dit is de reden dat ik ook heb besloten vooral naar deze vormen van wetgeving te kijken.

We zullen zien dat vrijwel alle wetgeving op dit gebied in Nederland privacygerelateerde wetgeving is die bescherming biedt voor de consument. Dit is voornamelijk voornamelijk terug te vinden in de Wet Bescherming Persoonsgegevens (WBP). Slechts een klein gedeelte gaat over de technische voorwaarden waaraan tags en readers moeten voldoen. Dit is vastgelegd in de Telecommunicatiewet. We kijken echter als eerste naar het Burgerlijk Wetboek. Hierin staat ook een artikel dat betrekking zou kunnen hebben op het gebruik van de RFID technologie of het gebruik van de persoonsgegevens, te weten de onrechtmatige daad. De onrechtmatige daad is geregeld in artikel 6:162 van het Nederlandse Burgerlijk Wetboek.

In lid 2 staat het volgende beschreven. "Als onrechtmatige daad worden aangemerkt een inbreuk op een recht" (art. 6:162 lid 2 bw).

In dit geval kan gedacht worden aan het recht op privacy dat een burger heeft. Dit recht kan geschaad worden als onbevoegden persoonsgegevens van klanten aflezen.

Nederland moet zich in haar wetgeving aanpassen aan de richtlijnen die de Europese Unie heeft gesteld met betrekking tot de bescherming van persoonsgegevens.



Afbeelding 8: Hiërarchische ladder van wetgeving

Europese wetgeving staat namelijk boven nationale wetten en als de Europese Unie een wet instelt dan moet Nederland haar wetgeving aanpassen zodat ze niet in strijd is met deze wet. In de afbeelding is te zien hoe de verhoudingen van het recht er internationaal uitzien.

### *5.1 Overzicht Europese richtlijnen betreffende privacy*

Als eerste zal er in dit hoofdstuk een overzicht te zien zijn van de richtlijnen van het Europees parlement en de Europese raad. De verschillende lidstaten, waaronder Nederland, hebben na het officiële bekendmaken van de richtlijnen vervolgens 3 jaar om de wetgeving om te zetten zodat de richtlijnen erin verwerkt zijn.

De eerste stap van het Europees Parlement en de Raad die over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens ging was Richtlijn 95/46/EG uit 1995. Deze richtlijn had betrekking op de verwerking van persoonsgegevens in het algemeen, over de plichten van de verantwoordelijken voor de verwerking, en de rechten van de betrokkenen.

Een verdere uitwerking van deze principes volgde met richtlijn 97/66/EG op 15 december 1997. Deze richtlijn ging over de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, die dus specifieke regels bevatte over de toepassing van richtlijn 95/46 in de telecommunicatiesector. De punten uit deze richtlijnen zijn terug te vinden in de telecommunicatiewet verder in dit hoofdstuk.

Richtlijn 2002/58/EG van het Europees Parlement en de Raad is het vervolg op Richtlijn 95/46/EG en richtlijn 97/66/EG. Deze richtlijn moet beschouwd worden als de vervanger van richtlijn 97/66/EG. In deze richtlijn wordt meer aandacht geschonken aan de ontwikkelingen op de markten van de technologieën voor elektronische-communicatiediensten, zodat ook bij het gebruik van deze diensten voorzien wordt in een voldoende mate van bescherming van persoonsgegevens en van de persoonlijke levenssfeer.

Deze richtlijn maakt ook deel uit van het zogenaamde "telecompakket", dat het nieuwe regelgevingskader vormt voor de sector van de elektronische communicatie. Het "telecompakket" omvat vier andere richtlijnen, namelijk over het algemeen kader, de toegang tot en de interconnectie van netwerken, machtigingen en licenties en de universele dienst.

In deze nieuwe richtlijn worden enkele min of meer gevoelige thema's behandeld, zoals het bewaren van verkeersgegevens om redenen van politietoezicht (opslaan van verkeersgegevens), het verzenden van ongevraagde berichten, het gebruik van

'spionagesoftware' ("cookies") en de opname van persoonsgegevens in openbare abonneelijsten.

Richtlijn 95/46/EG en Richtlijn 2002/58/EG zijn beide in de bijlage te vinden.

## *5.2 De Wet Bescherming Persoonsgegevens*

In tegenstelling tot wat veel mensen denken bestaat er geen 'Wet op de Privacy' (ECP, 2005). Er bestaat helemaal geen wetgeving met betrekking tot de RFID technologie. De enige wetgeving die hier betrekking op heeft is de Wet Bescherming Persoonsgegevens (WBP). Hierin zijn dan ook de richtlijnen van het Europees parlement en de raad verwerkt.

Maar ondanks dat er geen wet op de privacy is zegt het College Bescherming Persoonsgegevens dat ze geen probleem ziet voor RFID technologie in winkels, zolang de chip maar verwijderd of onklaar gemaakt wordt in de winkel ([www.rfid-technologie.nl](http://www.rfid-technologie.nl)). Dit is ook precies hetgeen er bij Selexyz gebeurt. Nadat het boek is afgerekend wordt door een medewerker van Selexyz de tag onklaar gemaakt. Hierdoor is het niet mogelijk gegevens van de tag buiten de winkel te lezen. Dit gebeurt vanuit het oogpunt van de wetgeving. Zo kan Selexyz niet het risico lopen de wet te overtreden of de consument te schaden.

Er bestaan daarnaast echter nog wel internationaal geldende regels voor privacy. Deze zijn vastgelegd in de U.N. Declaration of Rights Related to Privacy. Deze gaan over lichamelijke privacy, mentale privacy, cyber privacy, communicatie privacy en privacy met betrekking tot leefruimte. Hierin staan de rechten opgenomen die elk individu heeft met betrekking tot de leefruimte, vrijheid, veiligheid, meningsuiting et cetera (U.N. General Assembly, 1948). Ook de uitwerking hiervan is opgenomen in de bijlage.

De WBP is van toepassing op verwerkingen van persoonsgegevens. Een persoonsgegeven is iedere informatie betreffende een geïdentificeerde of identificeerbare persoon. Om van een persoonsgegeven te kunnen spreken moet de persoon op wie het gegeven betrekking heeft identificeerbaar zijn (WBP, 2001) .

De hoofdregel van de WBP op de RFID-technologie is als volgt: De WBP is op de RFID-technologie van toepassing op het moment dat persoonsgegevens van een betrokkene gedeeltelijk of geheel geautomatiseerd worden verwerkt.

De beginselen van behoorlijke gegevensverwerking zoals beschreven in de WBP zijn de volgende:

- Gegevensverwerking dient in overeenstemming met de wet en behoorlijk en zorgvuldig te gebeuren (artikel 6 WBP).

- Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld (artikel 7 WBP).
- Er bestaat een rechtmatige grondslag voor het verzamelen van persoonsgegevens (artikel 8 WBP).
- Persoonsgegevens worden niet verdere verwerkt op een wijze die onverenigbaar is met doeleinden van verkrijging (artikel 9 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 (artikel 11 WBP).
- Persoonsgegevens dienen met het oog op het doel van de verwerking juist en nauwkeurig te zijn (artikel 11 WBP).
- Persoonsgegevens dienen te worden beveiligd (artikelen 12, 13 en 14 WBP).
- Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor verwerkingsdoeleinden (artikel 10 WBP).

Verwerking van *gevoelige* persoonsgegevens is in principe niet toegestaan. In de wet worden uitzonderingen op dat verbod genoemd (artikelen 17 t/m 23 WBP). Deze zijn echter alleen op ziekenhuizen en hulpverleners van toepassing. De uitzondering die voor wat betreft RFID van belang is, is de "uitdrukkelijke toestemming van de betrokkene". Om te beoordelen of daarvan sprake is zijn de volgende drie punten van belang (Artz 1999):

1. De betrokkene moet zijn wil voor gegevensverwerking vrij en nadrukkelijk uiten. Hier mag op geen een manier druk op uitgeoefend zijn.
2. De wil voor gegevensverwerking moet betrekking hebben op een bepaalde of beperkte categorie van gegevensverwerking. Een zeer brede en onbepaalde machtiging tot het verwerken van gegevens is niet voldoende.
3. De betrokkene moet over noodzakelijke informatie kunnen beschikken om tot zijn keuze te komen. Daarom moet hij/zij voldoende geïnformeerd worden over de gegevensverwerking. Er moet bekend zijn welke aspecten van belang zijn voor de betrokkene. Daarnaast is er wel een eigen verantwoordelijkheid voor de betrokkene namelijk een zekere onderzoeksplicht.

Tot slot is er bij de verwerking van persoonsgegevens het volgende van belang: de betrokkene moet op de hoogte zijn van de geplande gegevensverwerking (artikelen 33 en 34 WBP) en zijn rechten moeten worden gerespecteerd. (artikelen 35 t/m 42 WBP).

- De betrokkene vóór het moment van de gegevensverwerking informatie verkrijgen over de identiteit van de partij die zijn gegevens verwerkt en de doeleinden van de verwerking. Indien het nodig is dient nadere informatie te worden verstrekt. Dit hangt af

van de aard van de gegevens, de manier van verkrijgen en de doeleinden waarvoor de gegevens gebruikt gaan worden (artikel 33 WBP).

- Als de persoonsgegevens niet worden verkregen bij de betrokkene dient de informatie uit punt 1 aan hem te worden medegedeeld op het moment van vastlegging van de gegevens of, wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking. In het geval dit onmogelijk blijkt of een onevenredige inspanning kost, geldt deze informatieplicht niet. Wel dient de verwerker van persoonsgegevens dan de herkomst van de gegevens vast te leggen. (artikel 34 WBP).

Samenvattend kan gesteld worden dat de WBP in haar tekst totaal niet technisch is. Ze is volledig van toepassing op het verwerken van persoonsgegevens met behulp van RFID-systemen (ECP, 2005).

### *5.3 De Telecommunicatiewet*

Naast de WBP is er nog één wet te vinden die betrekking heeft op de RFID technologie, de Telecommunicatiewet. Deze wet is meer technisch van aard dan de WBP. De telecommunicatiewet gaat over regels omtrent het gebruik van frequentieruimte zonder vergunning en de aanwijzing van categorieën radiozendapparaten.

In de telecommunicatiewet is de volgende regel vastgesteld: De gebruiker van frequentieruimte waarvoor geen vergunning is vereist, zorgt ervoor dat door het gebruik van het gewenste signaal van het radiozendapparaat geen storing of belemmering wordt veroorzaakt in andere radiozendapparaten dan wel in overige elektrische of elektronische apparaten (artikel 1 telecommunicatiewet).

De overige artikelen van deze wet gaan over technische zaken als de werkfrequentie en wat precies de kenmerken van een radiozendapparaat zijn. De voor RFID gangbare frequenties variëren van laag frequent tot zeer hoog frequent en zijn: 125KHz (Low Frequency), 13.56MHz (High Frequency), 860 tot 950 MHz (Ultra High Frequency), en 2.45GHz (microwave) (Schermer, 2005).

### *5.4 Conclusies*

Selexyz zal niet veel problemen krijgen met de RFID technologie verwacht ik. Waar Selexyz wél op moet letten zijn de persoonsgegevens van de klanten. Hier zijn door de WBP richtlijnen opgesteld waar Selexyz zich aan moet houden.

Ik denk dat het verstandig is als Selexyz de uitdrukkelijke toestemming van de klant vraagt voor het verwerken en bewaren van de persoonsgegevens. Pas als de klant deze uitdrukkelijke toestemming geeft mogen de gegevens verwerkt en bewaard worden. Op deze manier weten klanten dat er gegevens van ze bewaard worden en hebben ze hier mee ingestemd. Om het bewaren van klantgegevens aantrekkelijker te maken voor de klanten kan er voor gekozen worden om de klant voordeel te geven op de aankopen. Daarnaast kan Selexyz bezig blijven met het ontwikkelen van mechanismen en technieken die onverantwoord gebruik van bijvoorbeeld klantgegevens helpen voorkomen. Denk bijvoorbeeld aan het beter beveiligen van de klantgegevens zodat onbevoegden er niet bij kunnen. Bijvoorbeeld met codering en wachtwoorden. Er zullen altijd mensen blijven die de regels blijven overtreden om er voor zichzelf voordeel uit te halen.

Bij de RFID-toepassingen die enkel een uniek nummer bevatten (zoals bijvoorbeeld op de boeken) dient met name gekeken te worden naar de inrichting van de achterliggende bedrijfsprocessen en systemen. Is er sprake van een makkelijke koppeling tussen uniek nummer en persoonsgegevens, of is dit goed beveiligd? Van dat laatste moet dan logischerwijs sprake zijn.

Tot slot moet Selexyz de website goed beveiligen indien dit nu niet het geval is. Dit heb ik door de geringe tijd niet meer kunnen onderzoeken. Hier kunnen klanten namelijk ook gegevens achterlaten. Bijvoorbeeld als ze online een boek willen bestellen.

Van de Nederlandse websites voert 90 procent geen anti-spam beleid, bedoeld om te voorkomen dat persoonsgegevens zonder toestemming van de eigenaar gebruikt worden. Dat blijkt uit onderzoek dat *World IT Lawyers Network of Law Firms* heeft laten uitvoeren ([www.recht.nl](http://www.recht.nl)). Hierdoor kunnen klantgegevens van de klanten van Selexyz misschien wel zo van het internet gehaald worden.



## 6. Wat zijn de randvoorwaarden bij de invoeringswijze van RFID bij Selexyz?

### 6.1 Waar moet Selexyz rekening mee houden, en wat kan Selexyz het beste doen om de invoering van de RFID technologie zo voorspoedig mogelijk te laten verlopen?

In deze centrale vraag zal gekeken worden waar Selexyz rekening mee moet houden bij de invoering van de RFID technologie. Ook zal er aandacht zijn voor de klantenbenadering. Wat zijn verstandige punten waar Selexyz haar klanten op kan wijzen als ze voorlichting geeft over de RFID technologie. De eventuele angsten van de klanten moeten immers weggenomen worden en Selexyz zal daarnaast op voordelen moeten wijzen. We komen het onderzoeksdoel van dit verslag: Met welke randvoorwaarden moet men rekening mee houden zodat de RFID technologie zo goed mogelijk gaat werken. Dit is samen te vatten in een invoeringsstrategie. Nu de drie onderzoeksvragen beantwoord zijn kunnen we deze centrale vraag beter beantwoorden. De drie geformuleerde onderzoeksvragen waren immers variabelen die invloed hebben op de afhankelijke variabele, de hoofdvraag.

In dit hoofdstuk zullen de gevolgen van alle deelvragen nog eens kort doorgenomen worden en zal er gekeken worden wat de gevolgen voor Selexyz zijn.

We zagen in de eerste deelvraag dat klanten voordelen zien als de RFID technologie in een winkel toegepast gaat worden. De opgestelde voordelen zijn vervolgens door middel van de AHP methode gerangschikt in volgorde van belangrijkheid. Uit de resultaten van de AHP kwam naar voren dat de lagere prijzen van de boeken (51,5%) veruit het belangrijkste voordeel was dat klanten zien.



Afbeelding 9: RFID tags die op boeken geplaatst zijn

Op ruime afstand volgden het eenvoudig en snel bestellen van boeken die niet aanwezig zijn (22%) en de aankoopsgesties op basis van eerdere aankopen(14,3%). De minst belangrijke voordelen waren de kortere wachttijden (7,2%) en de persoonlijke reclame (4,8%).

Selexyz weet nu wat de belangrijkste voordelen zijn die de consumenten zien. Ze zal er nu voor moeten kiezen om haar klanten op deze voordelen te wijzen. Klanten moeten te weten komen dat prijzen kunnen dalen door lagere kosten in de logistieke keten en klanten moeten weten hoé makkelijk het wel niet is om een boek op te zoeken of te bestellen met de nieuwe technologie. Dit kan bijvoorbeeld verteld worden in

informatiefolders die in de winkel liggen, of medewerkers moeten de klanten hierop wijzen in de winkels.

Selexyz wil daarnaast graag innovatief genoemd worden. Selexyz kan dus ook beginnen over haar pioniersfunctie die ze vervuld bij de invoering van de RFID technologie. De technologie zal in de toekomst niet meer weg te denken zijn en hij is nu al in werking in enkele winkels van Selexyz. De klanten worden zo nieuwsgierig naar de technologie en willen ook weten hoe het werkt. Zo zal de invoering ook voorspoediger verlopen lijkt me.

Naast de hierboven genoemde voordelen, en de invloed hiervan, zijn er ongetwijfeld ook consumenten die bezwaren hebben tegen het toepassen van de RFID technologie door Selexyz. De meeste en grootste bezwaren zijn terug te vinden op het gebied van de privacy. Dus mochten klanten bezwaren hebben dan is dat in de meeste gevallen een bezwaar vanuit het privacyoogpunt. In de tweede onderzoeksvraag zijn de drie grootste privacyrisico's gegeven. De drie grootste privacyrisico's zijn het volgen van mensen, het categoriseren van mensen en het uitlezen van persoonsinformatie (Min EZ, 2006).

De relativeringen bij deze risico's zijn ook gegeven in de tweede onderzoeksvraag. Het volgen van mensen was om twee redenen niet mogelijk. Ten eerste heeft een tag reader een beperkt bereik en zul je, om iemand te willen volgen, duizenden tag readers nodig moeten hebben. Ten tweede moet diegene die iemand wil volgen ook toegang heeft tot de systemen en de achterliggende databases. De RFID-tag zendt namelijk geen persoonsgegevens uit maar slechts een unieke code. Toegang tot die systemen is vaak onmogelijk.

Het categoriseren van mensen is ook niet mogelijk. Om voor commerciële organisaties een interessant profiel op te stellen van consumenten moet er meer informatie beschikbaar zijn dan alleen een uniek nummer van een product dat een persoon bij zich draagt. Men moet dan ook over de persoonsgegevens beschikken. Toegang tot die systemen is, net zoals bij de vorige relativering, vaak onmogelijk. Tevens maken klanten nu ook al vaak gebruik van klantenkaarten. Hierbij worden ook persoonsgegevens opgeslagen. Wat dat betreft is er niets nieuws onder de zon.

Het uitlezen van de persoonsinformatie is niet mogelijk omdat er op de tags geen persoonsgegevens staan.

Mochten klanten met vragen of bezwaren bij Selexyz komen dan kan Selexyz de klanten wijzen op de relativeringen bij de privacyrisico's. Het geruststellen van de ongeruste klanten zou door voorlichting kunnen gebeuren. Hier valt voor Selexyz nog werk te verrichten. Zo kan men in informatiefolders of op beeldschermen een oproep doen aan bezorgde mensen. Die moeten bij de medewerkers of via een telefoonnummer informatie over de technologie kunnen krijgen en ze moeten er hun vragen kwijt kunnen. Ze

moeten het gevoel krijgen dat er wel naar ze geluisterd wordt. Selexyz kan de klanten erop wijzen dat de producten van Selexyz geen RFID tag meer bevatten als ze de winkel uit gaan. Die wordt immers vernietigd bij het afrekenen.

Selexyz kan ook de aanval openen en de privacyrisico's al direct relativeren in folders, brochures en voorlichtingen.

Tot slot moet Selexyz betere beveiligingsmaatregelen nemen zodat er géén onbevoegden bij de klantgegevens kunnen. Bijvoorbeeld door codering van gegevens of wachtwoorden. Deze gegevens behoren immers binnen Selexyz te blijven om privacyredenen. Op deze manier worden de genoemde privacyrisico's tot een minimum beperkt.

In de laatste deelvraag hebben we de wettelijke restricties behandeld. Te lezen was dat de meeste restricties te maken hebben met privacyrechtelijke aangelegenheden die vastgelegd zijn in de WBP. Hierin zijn ook veruit de meeste Europese richtlijnen verwerkt. Daarnaast bestaan de restricties nog voor een klein gedeelte uit technische bepalingen die over frequenties van readers gaan. De WBP is pas op de RFID technologie van toepassing als een persoonsgegeven van een betrokkene gedeeltelijk of geheel geautomatiseerd wordt verwerkt. Dus als er gegevens van een consument worden verwerkt.

Selexyz zal de klant uitdrukkelijke toestemming moeten vragen voor het verwerken en bewaren van de persoonsgegevens. Klanten weten nu dat er gegevens van ze bewaard worden en hebben ze hier mee ingestemd. Zo is het risico al een stuk verminderd door Selexyz. Gegevens worden immers niet 'stiekem' opgeslagen. Door klanten voordelen te geven als Selexyz de gegevens mag opslaan wordt het verstrekken van klantgegevens aantrekkelijker.

Daarnaast moet Selexyz ook op dit punt betere beveiligingsmaatregelen nemen. Op deze manier kunnen er géén onbevoegden bij de klantgegevens. Bijvoorbeeld door codering van gegevens of wachtwoorden. Deze gegevens behoren immers binnen Selexyz te blijven om privacyredenen.

Tot slot is het aan te raden om nog eens goed naar de website te kijken. Zoals al eerder gezegd voert 90% geen anti-spambeleid, bedoeld om te voorkomen dat persoonsgegevens zonder toestemming van de eigenaar gebruikt worden. De ICT afdeling binnen Selexyz zal dus eens goed naar de website moeten kijken om uit te zoeken of deze wel helemaal veilig is. Klanten kunnen namelijk ook online boeken bestellen en via deze manier klantgegevens aan Selexyz geven. Ook gegevens die via deze manier verkregen zijn behoren binnen Selexyz te blijven om privacyredenen.

## 6.2 Conclusie

Op deze manier is er rekening gehouden met alle mogelijke aspecten die een succesvolle invoering van de RFID technologie tegen kunnen gaan. Klanten worden geïnformeerd over de nieuwe technologie. Ze worden op de hoogte gesteld van de voordelen die het voor hen heeft en ze komen te weten waarom Selexyz de technologie invoert. Op deze manier is de keuze van Selexyz voor de RFID technologie onderbouwd.

Klanten die bezwaren hebben of problemen voorzien kunnen hun verhaal kwijt bij Selexyz en kunnen alsnog overtuigd worden wanneer de bezwaren of problemen ontkracht worden. Overigens ziet de helft van de Nederlandse consumenten die bekend zijn met RFID ziet voornamelijk voordelen. Slechts zeven procent ziet voornamelijk nadelen (Cappgemini 2005a). Het aantal klanten bij Selexyz dat nadelen naar aanleiding van deze gegevens niet al te groot zijn.

Tot slot is het zaak dat Selexyz voorzichtig en vertrouwelijk met de persoonsgegevens omgaat. Zolang ze dit maar doet zijn er vanuit het wettelijke oogpunt geen risico's te voorzien. De meeste wetten die van toepassing zijn gaan namelijk over de verwerking van de persoonsgegevens.

Alleen de medewerkers van Selexyz moeten de persoonsgegevens mogen inzien. Voor onbevoegden moet dit niet mogelijk zijn. Dus niet in een database in een winkel van Selexyz en ook niet via het internet.

## 7. Een communicatieplan voor Selexyz

We hebben in een deelvragen gezien wat de bezwaren van de consumenten tegen de RFID technologie zouden kunnen zijn. En we hebben in een deelvraag gezien welke voordelen de consumenten zien als de RFID technologie geïntroduceerd wordt.

In dit hoofdstuk zal ik adviezen en oplossingsrichtingen aan Selexyz geven die men kan gebruiken om de consumenten voor te lichten over de eventuele bezwaren tegen RFID technologie en de voordelen van de RFID technologie.

### *7.1 Manieren om consumentengedrag te beïnvloeden.*

Mochten de consumenten niet het gewenste gedrag vertonen volgens Selexyz, doordat ze bijvoorbeeld de nadelen zien en/of de voordelen niet zien, dan kan Selexyz er voor kiezen om het gedrag van de consumenten te beïnvloeden.

Er bestaan verschillende manieren om consumentengedrag te beïnvloeden. Mowen (1993) definieert consumentengedrag als de studie naar consumenten en naar de transitieprocessen die betrokken zijn bij het verkrijgen en consumeren van bepaalde goederen, diensten en ideeën.

De drie belangrijkste zijn het klassiek conditioneren, het instrumenteel conditioneren en het cognitief leren.

- Klassiek conditioneren: De consument leert door middel van associatie met een leuke of aangename situatie een merk kennen en ontwikkelt op basis van deze attitude met een positieve of negatieve houding (Shiffman & Kanuk, 1991).
- Voorbeeld: De klanten moeten de eerste dagen bij de hand genomen worden door de medewerkers van Selexyz. De klant kan, met hulp, zelf boeken leren bestellen, opzoeken en afrekenen met behulp van de RFID technologie. Op deze manier raakt men vertrouwd met de RFID technologie en de voordelen daarvan. Zo ontwikkelt zich een positieve houding bij de consument.
- Instrumenteel conditioneren: Bij instrumenteel conditioneren gaat men gedragingen die men wenselijk vindt belonen en gedragingen die men niet wenselijk vindt straffen. Op deze manier leert men conditioneren (Shiffman & Kanuk, 1991).
- Voorbeeld: Selexyz kan klanten die 'goed' gedrag vertonen gaan belonen. Bijvoorbeeld het geven van kortingen als mensen de SmartCard en RFID technologie gaan gebruiken. Ook kan gedacht worden aan het geven van cadeautjes als men bereid is een SmartCard aan te schaffen. Bijvoorbeeld een boek of een starttarief op de SmartCard van 7,50 euro. Straffen zal in deze zin moeilijk worden. Hierbij kan men

denken aan het niet geven van voordelen aan klanten die geen gebruik maken van de SmartCard en de RFID technologie.

- Cognitief leren: De cognitieve leertheorie gaat van het standpunt uit dat mensen informatie uit hun omgeving gebruiken om tot een oordeel te komen welk gedrag in een bepaalde situatie het beste is. (Bernstein et al, 1997).
- Voorbeeld: Hierbij kan Selexyz nadrukkelijk informatie geven over de RFID technologie. De klant zal deze informatie vervolgens verwerken en vervolgens een oordeel vormen over de RFID technologie. Het is nu dus zaak dat er positieve informatie over de RFID technologie naar buiten komt en negatieve informatie ontkracht wordt. Zo kan Selexyz de privacyrisico's ontkrachten want de relativeringen zijn bekend en men kan de klanten op de voordelen wijzen.

## *7.2 Adviezen*

Met deze manieren van beïnvloeding in ons achterhoofd kan Selexyz op verschillende manieren trachten het gedrag van de consument te beïnvloeden. Hieronder zijn 6 adviezen gegevens aan Selexyz die hierbij kunnen helpen. Tot slot zullen aan de hand van deze 6 adviezen enkele oplossingsrichtingen volgen.

### *Voorlichting RFID*

Het zou voor Selexyz aan te raden zijn om haar klanten een duidelijke voorlichting geven over RFID in zijn algemeenheid en de privacyrechtelijke aspecten ervan. Dit advies is zeer goed haalbaar voor Selexyz. Denk bijvoorbeeld aan het verspreiden van flyers onder klanten. Ook kan Selexyz folders in haar winkels leggen met nadere informatie over de RFID technologie.

Op deze manier komen de consumenten te weten dat de privacy die ze hebben in de wet beschermd is. Selexyz mag deze privacy dus niet afnemen. Een voorlichting hierover zal volgens mij aanzienlijk bijdragen aan de acceptatie van RFID.

### *Geruststellen*

Selexyz zou er daarnaast op moeten wijzen dat de RFID-tags die op de boeken zitten vernietigd worden als er afgerekend wordt. Op deze manier kan een klant niet gevolgd worden als hij de winkel uit gaat. Het volgen en 'uitscannen' van personen op afstand kan dus helemaal niet met de tags die op de boeken van Selexyz zitten. Op deze manier is er een onduidelijkheid verholpen, namelijk dat je met een RFID-tag overal te volgen zou zijn. Dit is bij Selexyz helemaal niet het geval. Het geruststellen van mensen is ook haalbaar. Hier zit wel een maar aan. Alle medewerkers van Selexyz moeten op de hoogte

van hoe de technologie precies werkt. Daarnaast moeten mensen ook naar de medewerkers van Selexyz toekomen als ze ongerust zijn. Dit gebeurt ook niet altijd. Bijvoorbeeld bij verlegen mensen. De effectiviteit zal lager liggen dan bij voorlichting.

#### *Open houding*

Ook zou Selexyz een open houding aan moeten nemen ten opzichte van haar klanten met betrekking tot de toepassing van RFID. Het hebben van een open houding is makkelijk haalbaar. Er moet gewoon eerlijk verteld worden of en waar de RFID technologie binnen Selexyz toegepast wordt.

Kennisgeving aan klanten is dus aan te raden en het kan daarnaast ook verstandig zijn om aanvullende informatie beschikbaar te stellen. Bijvoorbeeld recente ontwikkelingen op RFID gebied waar Selexyz zich mee bezig houdt. Een dergelijke open houding zal waarschijnlijk goed vallen bij de klanten. Zo krijgen klanten niet het gevoel dat er 'geheimen' voor hen verborgen blijven.

#### *Wijzen op voordelen*

Selexyz zou haar klanten tenslotte kunnen voorlichten over de voordelen die ze hebben als gevolg van de RFID technologie. Denk bijvoorbeeld maar aan de lagere kosten van de producten en de kortere wachttijden bij de kassa's. Men zou de klant ook bij de hand kunnen nemen de eerste dagen. Medewerkers leggen klanten dan uit hoe het bestellen van boeken snel en efficiënt kan gebeuren bij de KIP. Geen tijden meer wachten tot een boek besteld is maar binnen enkele dagen krijg je al een sms of email dat het bestelde boek er is. Zoals al eerder gezegd: Als de klanten zich bewust worden van de voordelen die ze hebben door de technologie zal ze de technologie eerder accepteren. Zeker als ze daarbij in ogenschouw nemen dat de privacy vrijwel niet geschaad kan worden door de RFID technologie.

Het wijzen op voordelen is makkelijk haalbaar. Selexyz zal er hooguit voor moeten zorgen dat ze de eerste tijd na de invoering wat meer medewerkers in haar winkel heeft. Dit omdat het voor de medewerkers een wat intensievere periode zal worden als mensen bij de hand moeten worden genomen. Daarentegen verwacht ik dat dit een hoge effectiviteit zal hebben. Als klanten het niet snappen wordt het ze uitgelegd en zo komen ze meteen de voordelen van de technologie te weten.

#### *Alternatieven*

Het is aan te raden om een alternatief plan achter de hand te houden mocht er iets mis gaan met de RFID technologie. Stel dat de RFID technologie niet goed werkt in een van de winkels van Selexyz of dat de techniek zeer negatief in het nieuws komt. Op dat moment moet Selexyz een 'plan B' hebben. Er moet in dat geval voor gezorgd worden

dat de winkels van Selexyz goed kunnen blijven functioneren zonder de RFID technologie. Het hebben van een alternatief is makkelijk haalbaar. Naast de RFID technologie moet de streepjescode nog een bepaalde periode actief blijven. Bijvoorbeeld een jaar. Daarna zijn de kinderziekten toch wel uit de technologie mag je verwachten.

#### *Binnen Selexyz gaan brainstormen*

Het laatste advies dat ik geef is dat men binnen Selexyz eens met zijn allen zou kunnen gaan brainstormen. Er zijn binnen Selexyz mensen die veel verstand hebben op het gebied van (RFID) technologie. Als deze mensen met elkaar gaan brainstormen komen ze misschien op ideeën waar ze zelf niet zouden zijn opgekomen. De haalbaarheid hiervan is groot. Het is niet moeilijk om eens alle mensen bij BGN ICT te laten brainstormen. De effectiviteit hiervan is onbekend. Het is van tevoren niet mogelijk te voorspellen met welke ideeën de mensen komen.

### *7.3 Oplossingsrichtingen voor Selexyz*

Met deze verschillende adviezen kan Selexyz verschillende richtingen op. Enkele oplossingsrichtingen die volgens mij gekozen kunnen worden zal ik hieronder beschrijven. Het is vervolgens aan Selexyz om de oplossingsrichting te kiezen die het beste bij haar past. Deze oplossingsrichtingen kunnen natuurlijk ook naar eigen inzicht gecombineerd worden.

- Selexyz kan de RFID technologie in meerdere winkels gaan invoeren en daarnaast de eerste tijd voor de klanten de mogelijkheid behouden om niet mee te doen aan het gebruik van de RFID technologie. De streepjescode zal dus nog actief moeten blijven. Er moet bij deze wijze van invoering voorlichting aan haar klanten gegeven door worden middel van flyers. Hierin kan Selexyz aan de klanten uitleggen wat de RFID technologie precies is, wat Selexyz met de RFID technologie van plan is en wat het voor de klant inhoudt. Er kan op de voordelen van de klanten gewezen worden en op de mogelijkheid om (nog) geen deel te nemen aan het gebruik van de RFID technologie.

Op deze manier is de klant gerustgesteld. Hij weet nu precies wat de veranderingen gaan worden en wat de gevolgen daarvan zijn. Ook weet hij dat, mits hij bezwaren heeft (nog) niet gedwongen wordt om deel te nemen aan de technologie.

- Er kan ook gekozen worden om de RFID technologie winkel voor winkel toe te passen. Op deze manier kan er per winkel gekeken worden waar er behoefte aan is. Het is niet ondenkbaar dat mensen in de Randstad anders reageren op de invoering van de RFID technologie dan mensen in het noorden van het land. Op



deze manier worden de kinderziekten verholpen en spelen deze 'ziekten' slechts in een paar winkels in plaats van alle winkels. Selexyz moet daarbij zorgen dat de klanten voorgelicht worden over de naderende toepassing van de RFID technologie in de winkel. De medewerkers moeten dan ook de kennis over de technologie hebben en weten wat er precies veranderd. Als er klanten met vragen komen kunnen deze beantwoord worden. Een dergelijke open houding zal door de klanten op prijs gesteld worden.

- Selexyz zou de invoering van de veranderingen in stappen kunnen doen. Zo zou de klantenkaart nu al in alle winkels die ze hebben verplicht ingevoerd moeten worden zodat de klanten al gewend raken aan het idee. De klanten raken dan al vertrouwd met het feit dat ze klantgegevens inleveren en in ruil daarvoor voordeel op boeken et cetera krijgen. Vervolgens kan men de RFID tags al op de boeken plaatsen en alleen de distributie via de RFID technologie laten lopen. Tot slot kan men na een paar jaar kan Selexyz er dan voor kiezen om de klantenkaart aan te laten sluiten op de RFID technologie. Op deze manier hoeft de klant niet voor én een klantenkaart én voor de RFID technologie te kiezen. De verandering wordt zo minder groot.
- Tot slot kan Selexyz mensen een soort kosteloos en vrijblijvend proefabonnement van de RFID technologie aanbieden voor degenen die dat willen. Mensen kunnen in dat geval een maand lang gratis een SmartCard gebruiken en alle voordelen zelf ervaren. Mensen moeten warm gemaakt worden voor de technologie dus men zou dan acties moeten starten. Bijvoorbeeld het 3<sup>e</sup> boek voor de halve prijs of het 4<sup>e</sup> boek gratis als de boeken door een SmartCardgebruiker gekocht worden. Men zou de klant die een SmartCard gebruikt ook een startbedrag op de kaart kunnen geven. Bijvoorbeeld 10 euro. Mensen willen op deze manier graag even kijken wat die nieuwe technologie precies is. Aan het einde van de maand kunnen klanten vervolgens zelf kiezen of ze de SmartCard willen houden of niet. Als ze dit niet willen worden alle klantgegevens vernietigd en heeft Selexyz geen gegevens meer van de klant. Mochten ze de SmartCard wel houden dan blijft men in aanmerking komen voor de voordelen die deze kaart met zich meebrengt.

Door gebruik te maken van deze adviezen en oplossingsrichtingen verwacht ik dat de RFID technologie eerder geaccepteerd zal worden door de klanten van Selexyz. Door een open houding, met veel informatie en een verwijzing naar de voordelen voor de klanten zou de RFID technologie toch geaccepteerd moeten worden. De klanten kunnen de techniek daarnaast ook zelf nog eens uittesten. Lijkt het ze niets dan kunnen ze hier ook

gemakkelijk van af. De grootste angst (privacy) wordt ondervangen door verschillende feiten zoals de passieve tags die Selexyz gebruikt en het feit dat de tags vernietigd worden. Daarnaast kan het de klant, kosteloos en zonder extra moeite, voordelen opleveren. En voordelen helpen vaak mee om nadelen naar de achtergrond te dringen.

## 8. Literatuurlijst

### *Boeken / Artikelen*

- Ministerie van Economische Zaken, *Notitie 'RFID in Nederland'*, september 2006, pp. 3
- Ministerie van Economische Zaken, *Notitie 'RFID in Nederland'*, november 2006, pp. 9-10
- J. Vink, *BGN Selexyz RFID Item Level Case*, 2006, pp. 1
- H. Heerkens, *Methodologische checklist*, 2004, pp. 3, 12
- Shadish, Cook & Campbell, *Experimental and Quasi-Experimental Designs*, 2002, pp.172-177
- E. Rogers, *Diffusion of Innovation 4th edition*, 1995 (oorspronkelijk uit 1962), The Free Press, New York, pp 161  
182, 212, 263 - 265
- Ministerie van Economische Zaken, *Notitie 'RFID in Nederland'*, 2006, pp. 3
- P. Morville, *Ambient findability; What We Find Changes Who We Become*, 2005, O'Reilly Media, pp 4 – 7, 43 – 63
- B. Hardgrave en R. Miller, *The Myths and Realities of RFID in: International Journal of Global Logistics & Supply Chain Management*, 2006, University of Arkansas, pp. 4, 7
- ECP, *Privacyrechtelijke aspecten van RFID*, 2005, Efficiënta Offsetdrukkerij BV, pp 16, 22, 39
- Capgemini, *RFID in de praktijk*, In: ECP Privacyrechtelijke aspecten van RFID, 2005
- WBP, 2001, artikel 1, 6 tm 14, 17 tm 23, 33 tm 42
- Richtlijnen Europese Gemeenschap, 1995, richtlijn 95/46
- M.J.T. Artz, *Koning Klant, het gebruik van klantgegevens voor marketingdoeleinden*, uit: Achtergrondstudies en Verkenningen nr 14, 1999, Den Haag, p 16
- B. Schermer, *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen*, 2005, Den Haag, pp 16
- D.A. Bernstein, A. Clarke-Steward, E.J Roy & C.D. Wickens, *Psychology* (4e editie), 1997 New York, pp 38-46
- L. Shiffman & L. Kanuk, *Consumer behaviour*, 1991, Englewood cliffs, pp 28-32
- J.C. Mowen, *Judgment calls: High stakes decisions in a risky world*, 1993 New York, pp 4
- T.L. Saaty, *Multicriteria Decision Making: The Analytic Hierarchy Process, Vol. 1, AHP Series*, 1990, pp 492-504, RWS Publications, Pittsburgh
- J. Holvast & M. Koers, *Informatiebeveiliging*, Editie 2, maart 2003, pp 1-3
- J. Holvast, *Privacy & Informatie*, 3<sup>e</sup> jaargang nummer 2, april 2000, pp 71-75

## Websites

- [Http://www.zibb.nl/retail/food/artikel\\_start.asp/artnr/728978/index.html](http://www.zibb.nl/retail/food/artikel_start.asp/artnr/728978/index.html) (bezocht op 14 mei 2007)
- <http://rfid.emerce.nl/2004/06/index.html> (bezocht op 21 mei 2007)
- [http://www.rfid-technologie.nl/stakeholders\\_rfid.php](http://www.rfid-technologie.nl/stakeholders_rfid.php) (bezocht op 6 juni 2007)
- <http://www.recht.nl/artikel/index.html?nid=12100&marker=20337> (bezocht op 2 juli 2007)

## Afbeeldingen

Afbeelding 1: PowerPoint presentatie RFID presentatie Selexyz, *Multi Channel Strategy, Beyond RFID*, 7 november 2006, pp 20

Afbeelding 2: Ministerie van Economische Zaken, *Notitie 'RFID in Nederland'*, september 2006, pp 5

Afbeelding 3: PowerPoint presentatie RFID presentatie Selexyz, *Multi Channel Strategy, Beyond RFID*, 7 november 2006, pp 9

Afbeelding 5: PowerPoint presentatie RFID presentatie Selexyz, *Multi Channel Strategy, Beyond RFID*, 7 november 2006, pp 17

Afbeelding 6: PowerPoint presentatie RFID presentatie Selexyz, *Multi Channel Strategy, Beyond RFID*, 7 november 2006, pp 17

Afbeelding 7: C. Walks, *Pervasive computing: The Evolution of Accessibility to Information*, 2003, pp 12

Afbeelding 8: J.S. van Veen, *De veranderingen door de RFID technologie bij Selexyz*, 2007, pp 24

Afbeelding 9: PowerPoint presentatie RFID presentatie Selexyz, *Multi Channel Strategy, Beyond RFID*, 7 november 2006, pp 3

## Bijlagen

### Bijlage 1 Internationale wetgeving (algemeen)

Op internationaal niveau zijn er diverse verdragen waarin het recht op privacy is vastgelegd.

#### *-Universele Verklaring van de Rechten van de Mens*

Op 10 december 1948 is door de Algemene Vergadering van de Verenigde Naties de Universele Verklaring van de Rechten van de Mens aangenomen. De lidstaten van de Verenigde Naties verplichten zich door middel van de Verklaring de rechten van de mens zo goed mogelijk te waarborgen.

De Universele Verklaring is niet bindend, met andere woorden de Verklaring kent geen speciaal handhavingmechanisme. Het is veeleer een intentieverklaring van de deelnemende landen om binnen hun territorium de mensenrechten te respecteren en op internationaal niveau te streven naar een betere waarborging van deze rechten.

Artikel 12 van de Verklaring ziet op de bescherming van de persoonlijke levenssfeer: Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.

#### *-Het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR)*

Het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) werd op 16 december 1966 aangenomen door de Algemene Vergadering van de Verenigde Naties en werd op 23 maart 1976 officieel van kracht. Het IVBPR betreft een uitwerking van de rechten opgesomd in de Universele Verklaring van de Rechten van de Mens. In tegenstelling tot de Universele Verklaring is het IVBPR wel bindend. Een Comité ziet toe op de naleving van de in het verdrag opgesomde rechten en plichten.

Artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten stelt dat:

‘Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.’ en dat een ieder recht heeft op bescherming door de wet tegen zodanige inmenging of aantasting.

#### *-EVRM*

Het voor Nederland belangrijkste verdrag op het gebied van de bescherming van de mensenrechten is het Verdrag tot de Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM).

Op 4 november 1950 is dit verdrag aangenomen door de Raad van Europa.

Artikel 8 EVRM ziet op de bescherming van de persoonlijke levenssfeer. Het is de Europese

tegenhanger van artikel 10 Grondwet. De artikelen lijken sterk op elkaar en zijn beide techniekonafhankelijk. Artikel 8 EVRM luidt als volgt:

1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economische welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

### Bijlage 2 regelgeving informatiele privacy

Naast wetgeving zijn er diverse regelgevende initiatieven op het gebied van privacy in het algemeen en RFID in het bijzonder. Hoewel deze initiatieven niet de status hebben van wetgeving kunnen ze wel van groot belang zijn. Belangrijke regelgeving met

betrekking tot privacy zijn de Fair Information Practice Principles en de OECD Privacy Guidelines. De OECD Guidelines bevatten belangrijke beginselen op het gebied van kwaliteit, doelspecificatie, doelbinding, beveiligingswaarborgen, transparantie, aansprakelijkheid en recht op inzage, correctie en verzet. Deze beginselen zijn van grote invloed geweest op de ontwikkeling van privacywetgeving met name binnen de Europese Unie.

#### *-Fair Information Practice Principles*

De Fair Information Practice Principles gepubliceerd door de US Department of Health, Education and Welfare zijn:

- Er mogen geen systemen zijn voor de verwerking van persoonsgegevens waarvan het bestaan geheim is.
- Het moet voor een persoon mogelijk zijn om kennis te nemen van de informatie die over hem of haar verzameld is en hoe deze informatie verwerkt wordt.
- Het moet voor een persoon mogelijk zijn om te voorkomen dat informatie betreffende zijn/haar persoon zonder toestemming aangewend of verstrekt wordt voor een doel anders dan de oorspronkelijke verwerking.
- Het moet voor een persoon mogelijk zijn om zijn/haar persoonsgegevens te verbeteren of aan te vullen.
- Elke organisatie die verantwoordelijk is voor het genereren, onderhouden, gebruiken, verstrekken of anderszins verwerken van persoonsgegevens moet zorg dragen voor de betrouwbaarheid van deze persoonsgegevens, voor het doel van de verwerking en maatregelen nemen om misbruik van deze persoonsgegevens te voorkomen.

#### *-OECD Privacy Guidelines*

De OECD Privacy Guidelines zijn in 1980 binnen de OECD (OESO) opgesteld. De Guidelines vormen een belangrijk richtsnoer voor de verwerking van persoonsgegevens en staan aan de basis van diverse internationale wetgevingsinitiatieven. De Guidelines leggen een aantal principes neer welke hieronder opgesomd staan:

##### • Collection limitation principle

Deze bepaling stelt dat er een limiet is aan de hoeveelheid gegevens die over een persoon verzameld mogen worden en dat deze data op rechtmatige en eerlijke wijze verkregen moet worden, waar noodzakelijk met de wetenschap of toestemming van de betrokkene.

##### • Data quality principle

Deze bepaling stelt dat persoonsgegevens noodzakelijk moeten zijn voor het doel waartoe ze verwerkt worden en voor dit doel compleet, nauwkeurig en up-to-date moeten zijn.

##### • Purpose Specification principle

Deze bepaling stelt dat het doel waartoe persoonsgegevens verzameld worden niet later vermeld dient te worden dan het moment van verkrijging, en dat de persoonsgegevens enkel en alleen mogen worden verwerkt ten behoeve van dit doel, of doelen die met het oorspronkelijke doel verenigbaar zijn.

##### • Use limitation principle

Deze bepaling stelt dat persoonsgegevens niet openbaar mogen worden gemaakt, verstrekt of anderszins gebruikt anders dan in overeenstemming met het purpose specification principle (doelbindingscriterium). Een uitzondering op deze regel is enkel mogelijk met de toestemming van de betrokkene of bij de wet voorzien.

##### • Security safeguards principle

Deze bepaling stelt dat er adequate veiligheidsmaatregelen genomen dienen te worden om

persoonsgegevens te beschermen tegen ongeoorloofde toegang, vernietiging, gebruik, aanpassing of openbaring.

##### • Openness principle

Deze bepaling stelt dat er een algemeen beleid van openheid dient te zijn met betrekking tot

ontwikkelingen, toepassingen en beleidsvorming op het gebied van de verwerking van

persoonsgegevens. Het moet in afdoende mate mogelijk zijn om het bestaan en de aard van

persoonsgegevens vast te stellen, alsmede de doelen voor het gebruik van persoonsgegevens. Verder moet het mogelijk zijn om de vestigingsplaats en de identiteit van de verantwoordelijke voor de verwerking vast te stellen.

- Individual participation principle

Deze bepaling geeft de betrokkene een aantal rechten te weten:

a) Het recht om van een verantwoordelijke te vernemen of deze persoonsgegevens over de

betrokkene heeft.

b) Het recht om informatie te krijgen over zijn persoonsgegevens:

i) binnen een redelijke termijn;

ii) -indien niet gratis- tegen een redelijk bedrag;

iii) op een redelijke manier;

iv) in een formaat dat duidelijk te begrijpen is.

c) Het recht op motivatie indien de rechten onder a) en b) niet gehonoreerd kunnen worden en de mogelijkheid om zich tegen deze weigering te verzetten.

d) Het recht om in verzet te gaan tegen de verwerking van zijn persoonsgegevens en indien dit verzet gegrond wordt geacht het recht om de persoonsgegevens te wissen, rectificeren,

aanvullen of completeren.

- Accountability principle

Deze bepaling stelt dat de verantwoordelijke aansprakelijk is voor het naleven van alle voorgaande bepalingen.

### **Bijlage 3 RFID specifieke (zelf)regulering**

In dit hoofdstuk zal wet- en regelgeving met betrekking tot privacy in het algemeen en RFID in het bijzonder aan de orde komen. De eerste twee paragrafen bieden enige achtergrondinformatie over internationale verdragen en regelgeving. Het is van belang hier kort bij stil te staan omdat geldende wetten regelgeving vaak mede hierop is gebaseerd. Vervolgens worden relevante Europese richtlijnen en Nederlandse wetgeving behandeld. Voor de volledigheid is ook specifieke RFID-wetgeving uit de Verenigde Staten opgenomen.

Naast algemene wet- en regelgeving op het gebied van informationele privacy wordt er ook hard gewerkt aan RFID specifieke regulering. Hieronder worden de belangrijkste initiatieven opgesomd.

#### *-EPC guidelines*

Als beheerder van de EPC standaard heeft EPCGlobal een aantal richtlijnen voor het gebruik van EPC opgesteld. Deze richtlijnen dienen als aanvulling op reeds bestaande nationale en internationale wet- en regelgeving. De EPC Guidelines moeten het vertrouwen in het gebruik van de EPC en het EPC netwerk stimuleren. De Guidelines bevatten vier kernpunten:

- Consumer Notice

Consumenten moeten op de hoogte worden gesteld van de aanwezigheid van EPC RFID-tags. Hiertoe dient een vermelding te worden opgenomen op het product of de verpakking.

- Consumer Choice

Consumenten moeten geïnformeerd worden over de mogelijkheden om EPC RFID-tags te verwijderen of uit te schakelen wanneer deze gekocht worden.

- Consumer Education

Consumenten moet de mogelijkheid worden geboden om snel en makkelijk duidelijke informatie te krijgen over EPC, de toepassingen ervan en toekomstige ontwikkelingen op het gebied van EPC.

- Record Use, Retention and Security

Het verwerken van (persoons)gegevens gegenereerd door het EPC-systeem dient in overeenstemming te zijn met alle toepasselijke wet- en regelgeving. Bedrijven die

gebruik maken van EPC dienen kenbaar te maken (bijvoorbeeld door publicatie op de website) wat hun beleid is met betrekking tot de verwerking en bescherming van persoonsgegevens, met name die (persoons)gegevens die gegenereerd en/of verwerkt worden door het EPC-systeem.

#### *-RFID Bill of Rights*

In oktober 2002 verscheen in Technology Review van de hand van Simson Garfinkel het artikel 'An RFID Bill of Rights'. In dit artikel schetste Garfinkel de mogelijke gevaren voor de privacy van burgers als gevolg van het gebruik van RFID. Hij stelt een 'Bill of Rights' voor waarin een aantal consumentenrechten zijn vastgelegd. Het gaat om de volgende rechten:

- het recht om te weten of een product een RFID-tag bevat;
- het recht om RFID-tags uit te schakelen of te verwijderen wanneer een product gekocht wordt;
- het recht om van diensten gebruik te maken zonder RFID-tags, daar waar deze normaliter wel van RFID gebruik maken.
- het recht om kennis te nemen van de in een tag opgeslagen informatie;
- het recht om te weten wanneer, waar en waarom tags gelezen worden.

#### *-ICDPPC Resolution on Radio-Frequency Identification*

Op 20 november 2003 is door de International Conference of Data Protection & Privacy Commissioners een resolutie aangenomen met betrekking tot het verantwoord gebruik van RFID. De resolutie bevat de volgende punten:

- Elke verantwoordelijke moet, alvorens over te gaan tot de introductie van een RFID-systeem dat persoonsgegevens verwerkt, alle mogelijke alternatieven overwegen waarmee hetzelfde doel kan worden bereikt zonder de verwerking van persoonsgegevens.
- Als de verantwoordelijke kan aantonen dat de verwerking van persoonsgegevens door middel van een RFID-systeem noodzakelijk is, dan dient deze verwerking open en transparant te geschieden.
- Persoonsgegevens mogen alleen verwerkt worden voor het doel waartoe ze verkregen zijn en mogen alleen bewaard worden zolang dit noodzakelijk is voor het doel waartoe de persoonsgegevens verkregen zijn.
- Wanneer een RFID-tag in het bezit van een individu komt, dan moet deze de mogelijkheid worden geboden de tag onschadelijk te maken en/of de daarop vastgelegde data te vernietigen.

#### **Bijlage 4 Voorgestelde RFID specifieke wetgeving**

In de Verenigde Staten (waar de toepassing van RFID verder gevorderd is dan in Europa) zijn reeds drie formele wetgevingsinitiatieven genomen om het gebruik van RFID in goede banen te leiden. De voorstellen zijns deels ingegeven door het werk van consumentenorganisatie CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) die voor dit doel zelfs een eigen model voor een wet hebben gemaakt: de CASPIAN RFID Right to Know Act.<sup>40</sup> Overigens zijn alle wetsvoorstellen tot op heden gestrand in het wetgevingstraject. De voornaamste reden hiervoor is dat beleidsmakers niet de ontwikkeling van een veelbelovende technologie nodeloos willen belemmeren door de introductie van starre, premature wetgeving.

#### *-CASPIAN RFID Right to Know Act*

Naast zelfregulerende initiatieven geïnitieerd door marktpartijen die RFID willen gaan gebruiken, is in de Verenigde Staten door consumenten belangengroepering CASPIAN een model voor een wet opgesteld welke het gebruik van RFID moet reguleren.

De wet, welke de US Code zou moeten amenderen kent de volgende hoofdpunten:

- De verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat.



- Een bepaling die het aanbrengen van een onduidelijk label dat aangeeft dat een product een RFID-tag bevat bedreigt met sancties gelijk aan die gelden voor het verkeerd of niet labelen van producten.
- Het verbod voor bedrijven om persoonsgegevens te koppelen aan informatie vastgelegd in individuele RFID-tags, anders dan hetgeen noodzakelijk is voor voorraadbeheer.
- Een verbod voor bedrijven om persoonsgegevens in samenhang met identificerende informatie uit een RFID-tag te verstrekken aan derden.
- Een aanwijzing aan de Federal Trade Commission om richtlijnen voor bedrijven op te stellen ter waarborging van de integriteit, vertrouwelijkheid en beveiliging van persoonsgegevens.
- Een aanwijzing aan de Federal Trade Commission om te waarborgen dat gegevens verkregen uit RFID-tags geen personen kunnen identificeren.
- Een aanwijzing aan de Federal Trade Commission om individuen te beschermen tegen mogelijke (toekomstige) bedreigingen voor de veiligheid van persoonsgegevens en negatieve gevolgen voor het individu die hier het gevolg van kunnen zijn.
- Een aanwijzing aan de Federal Trade Commission om burgers en bedrijven voor te lichten over het gebruik van RFID en de mogelijke negatieve gevolgen die dit kan hebben voor de privacy van de burger.

De RFID Right to Know Act of 2003 heeft als voorbeeld gediend voor de wetgevende initiatieven op deelstaat niveau. Deze wetsvoorstellen zijn minder vergaand dan het origineel.

#### *RFID Right to Know Act 2004 (California)*

In februari 2004 is door Senator Bowen in California een wetsvoorstel ingediend dat het gebruik van RFID-systemen moet reguleren. In tegenstelling tot het wetsvoorstel van CASPIAN richt de aanpassing zich niet op federale wetgeving, maar op aanpassing van de wet in de deelstaat California. Inmiddels heeft het voorstel een aantal amendementen ondergaan en is het in april 2004 door de State Senate goedgekeurd. Eind juni 2004 is het wetsvoorstel echter verworpen in de State Assembly. Het wetsvoorstel bevatte de volgende punten: Wanneer een RFID-systeem gebruik maakt van RFID-tags gekoppeld aan consumentenproducten of een reader die het mogelijk maakt om door het lezen van RFID-tags op consumentenproducten informatie te verzamelen, opslaan, gebruiken of delen die kan worden gebruikt om een persoon te identificeren, is voor een bedrijf niet toegestaan dit systeem te gebruiken tenzij:

- De reikwijdte van de verzamelde informatie niet verder gaat dan bij wet wordt toegestaan;
  - De informatie door een klant aan het bedrijf wordt verstrekt om de afhandeling van een overeenkomst met betrekking tot het kopen of huren van een product met RFID-tag mogelijk te maken;
  - De informatie niet verzameld wordt vóór het moment dat de klant daadwerkelijk de overeenkomst tot het kopen of huren van een product met RFID-tag aangaat en na het moment dat de overeenkomst is afgehandeld;
  - De informatie alleen betrekking heeft op de klant die daadwerkelijk een product met RFID-tag wil kopen of huren en alleen met betrekking tot dat specifieke product<sup>44</sup>.
- Voor een bibliotheek gelden dezelfde voorwaarden, maar dan met betrekking tot de boeken die worden geleend.

Een belangrijke commissie in dit wetsvoorstel is de afwezigheid van een definitie van het begrip RFID.

Hoewel senator Bowen te kennen heeft gegeven dat de wetgeving alleen van toepassing is op die RFIDsystemen waarmee persoonsgegevens verwerkt worden, betekent de afwezigheid van een definitie veel onzekerheid over de precieze reikwijdte en invulling van de wet.

#### *-RFID Right to Know Act 2004 (Utah)*

In Utah is ook een wetsvoorstel ingediend om het gebruik van RFID te reguleren, maar dat voorstel is vooralsnog van de baan. Nadat de wet goedgekeurd was door de Business and Labor Committee en het Huis van Afgevaardigden van Utah, verliep de indieningstermijn bij de Senaat van Utah. Waarschijnlijk zal het voorstel opnieuw worden ingediend op een later tijdstip. Het voorstel bevatte de volgende punten:

- De verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat, of indien dit niet mogelijk is, een waarschuwing nabij het product (bijvoorbeeld op het schap).
- De verplichting om RFID-tags uit te schakelen bij het verlaten van de winkel, tenzij een consument uitdrukkelijk aangeeft de tag actief te willen houden.

*-RFID Right to Know Act 2004 (Missouri)*

Ook in de staat Missouri is een RFID Right to Know Act ingediend. Het voorstel kent slechts één bepaling: de verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat. Ook dit voorstel is gestrand in het wetgevingstraject.

**Bijlage 5 belangrijkste punten uit de Richtlijn 95/46/EG**

Richtlijn 95/46/EG van het Europese 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

Deze richtlijn is van toepassing op gegevens die worden verwerkt met geautomatiseerde middelen (bijvoorbeeld een klantendatabase), en op gegevens die zijn opgenomen of bestemd zijn om te worden opgenomen in een niet geautomatiseerd bestand (traditionele papieren bestanden).

De richtlijn is niet van toepassing op de verwerking van gegevens:

- die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht;
- die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt, zoals de openbare veiligheid, defensie of de veiligheid van de staat.

De richtlijn beoogt de rechten en vrijheden van personen te beschermen bij de verwerking van persoonsgegevens door leidende beginselen vast te stellen waarin de rechtmatigheid van deze verwerking wordt bepaald. Deze beginselen hebben betrekking op:

- de kwaliteit van de gegevens: persoonsgegevens moeten met name eerlijk en rechtmatig worden verwerkt en voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen. Zij moeten bovendien nauwkeurig zijn en, zo nodig, worden bijgewerkt;
- de toelaatbaarheid van gegevensverwerking: de verwerking van persoonsgegevens mag slechts geschieden indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend of indien de verwerking noodzakelijk is:
  - voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
  - om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is;
  - ter vrijwaring van een vitaal belang van de betrokkene;

- voor de vervulling van een taak van algemeen belang; of
  - voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke;
- de bijzondere categorieën verwerkingen: moet worden verboden de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen. Met betrekking tot deze bepaling wordt op enkele punten voorbehoud gemaakt, bijvoorbeeld wanneer de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of voor de doeleinden van preventieve geneeskunde of medische diagnose;
- de informatieverstrekking aan de betrokkenen: de voor de verwerking verantwoordelijke moet aan de betrokkene, bij wie de betrokkene zelf betreffende gegevens worden verkregen, een aantal inlichtingen verstrekken (identiteit van de voor de verwerking verantwoordelijke, doeleinden van de verwerking, ontvangers van de gegevens, enz.);
- hun recht op toegang tot de gegevens: elke betrokkene moet het recht hebben om van de voor de verwerking verantwoordelijke te verkrijgen:
- uitsluitel omtrent het al dan niet bestaan van verwerkingen van hem betreffende gegevens en verstrekking van de gegevens die zijn verwerkt;
  - de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens, alsmede kennisgeving van deze wijzigingen aan derden aan wie de gegevens zijn verstrekt;
- de uitzonderingen en beperkingen: de reikwijdte van de beginselen betreffende de kwaliteit van de gegevens, de informatieverstrekking aan de betrokkene, het recht van toegang en de openbaarheid van de verwerkingen kan worden beperkt ter vrijwaring van, onder meer, de veiligheid van de staat, de landsverdediging, de openbare veiligheid, de vervolging van strafbare feiten, een belangrijk economisch en financieel belang van een lidstaat of van de EU, of de bescherming van de betrokkene;
- hun recht van verzet tegen de gegevensverwerking: de betrokkene moet het recht hebben zich om gerechtvaardigde redenen ertegen te verzetten dat hem betreffende gegevens het voorwerp van een verwerking vormen. Hij moet zich tevens kunnen verzetten, op verzoek en kosteloos, tegen de voorgenomen verwerking van gegevens met het oog op direct marketing. Ten slotte moet hij worden ingelicht voordat gegevens aan derden worden verstrekt voor direct marketing en moet hij het recht hebben zich tegen deze verstrekking te verzetten;
- de vertrouwelijkheid en de beveiliging van de verwerking: eenieder die handelt onder het gezag van de voor de verwerking verantwoordelijke of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de voor de verwerking verantwoordelijke verwerken. Voorts moet de voor de verwerking verantwoordelijke passende maatregelen ten uitvoer leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang;
- de aanmelding van de verwerkingen bij een toezichthoudende autoriteit: de voor de verwerking verantwoordelijke moet bij de nationale toezichthoudende autoriteit aanmelding doen voordat wordt overgegaan tot een verwerking van gegevens. Na ontvangst van de aanmelding worden door de toezichthoudende autoriteit voorafgaande

onderzoeken uitgevoerd naar eventuele risico's voor de rechten en vrijheden van de betrokkenen. Er moet worden gezorgd voor de openbaarheid van de verwerkingen en de toezichthoudende autoriteiten moeten een register van de aangemelde verwerkingen bijhouden.

Eenieder moet zich tot de rechter kunnen wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht, geschonden worden. Bovendien heeft eenieder die schade heeft geleden ten gevolge van een onrechtmatige verwerking van zijn persoonsgegevens, het recht vergoeding van de geleden schade te verkrijgen.

De doorgifte van persoonsgegevens van een lidstaat naar een derde land dat een passend beschermingsniveau waarborgt, is toegestaan. De doorgifte naar een derde land dat geen passend beschermingsniveau waarborgt, is echter niet toegestaan, met uitzondering van een aantal afwijkingen die beperkend worden opgesomd.

De richtlijn beoogt de opstelling van nationale en communautaire gedragscodes aan te moedigen die bestemd zijn om bij te dragen tot de juiste toepassing van de nationale en communautaire bepalingen.

Iedere lidstaat bepaalt dat een of meer onafhankelijke autoriteiten worden belast met het toezicht op de toepassing op zijn grondgebied van de ter uitvoering van deze richtlijn door de lidstaten vastgestelde bepalingen.

Er wordt een Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens ingesteld die bestaat uit vertegenwoordigers van de nationale toezichthoudende autoriteiten, vertegenwoordigers van de voor de communautaire instellingen en organen opgerichte autoriteiten en een vertegenwoordiger van de Commissie.

#### **Bijlage 6 belangrijkste punten uit de Richtlijn 2002/58/EG**

Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002. Dit betreft de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn "privacy en elektronische communicatie").

Richtlijn 2002/58/EG maakt deel uit van het zogenaamde "telecompakket", dat het nieuwe regelgevingskader vormt voor de sector van de elektronische communicatie. Het "telecompakket" omvat vier andere richtlijnen, namelijk over het algemeen kader, de toegang tot en de interconnectie van netwerken, machtigingen en licenties en de universele dienst.

In deze richtlijn worden enkele min of meer gevoelige thema's behandeld, zoals het bewaren van verkeersgegevens door de lidstaten om redenen van politietoezicht (opslaan van verkeersgegevens), het verzenden van ongevraagde berichten, het gebruik van "spionagesoftware" ("cookies") en de opname van persoonsgegevens in openbare abonneelijsten

-Vertrouwelijk karakter van de communicatie

In de richtlijn wordt het basisbeginsel in herinnering gebracht dat de lidstaten door hun nationale wetgeving het vertrouwelijke karakter van de communicatie via openbare elektronische communicatienetwerken moeten garanderen. Zij moeten met name af luisteren, aftappen en opslaan van communicatie verbieden, indien de betrokken gebruikers hiervoor geen toestemming hebben verleend.

Opslaan van verkeersgegevens

Wat het gevoelige punt van het bijhouden van gegevens betreft, wordt in de richtlijn bepaald dat de lidstaten de gegevensbescherming slechts mogen opheffen om het

onderzoek van strafbare feiten mogelijk te maken of de openbare veiligheid, de landsverdediging en de staatsveiligheid te waarborgen. Een dergelijke maatregel mag pas worden genomen wanneer dat "in een democratische samenleving noodzakelijk, redelijk en proportioneel is".

-Ongevraagde elektronische communicatie ("spamming")

In de richtlijn wordt gekozen voor een "opt-in"-aanpak met betrekking tot ongevraagde elektronische communicatie om commerciële doeleinden. Dit houdt in dat de gebruikers van te voren met de ontvangst van dergelijke berichten moeten hebben ingestemd. Een dergelijk "opt-in"-systeem geldt ook voor SMS-berichten en andere elektronische berichten die op om het even welke vaste of mobiele eindapparatuur kunnen worden ontvangen.

-Spionagesoftware ("cookies")

Cookies zijn verborgen gegevens die worden uitgewisseld tussen een internetgebruiker en de webserver en die worden bewaard op de harde schijf van de gebruiker. Dergelijke gegevens waren oorspronkelijk bedoeld om gemakkelijk informatie over twee verbindingen te bewaren. Zij zijn echter ook een instrument waarmee de activiteit van een internaut kan worden bespioneerd.

In de richtlijn is bepaald dat de gebruikers over de mogelijkheid moeten beschikken om te weigeren dat een cooky of soortgelijke voorziening op hun eindapparatuur wordt opgeslagen. Om hen daartoe in de gelegenheid te stellen, moeten zij duidelijke en nauwkeurige informatie ontvangen over het doel en de rol van dergelijke cookies.

Openbare abonneelijsten

De Europese burgers moeten van te voren toestemming verlenen voor opname van hun telefoonnummer (vast dan wel mobiel), hun e-mail-adres en hun postadres in een openbare abonneelijst.

-Door Richtlijn 2006/24/EG aangebrachte wijzigingen

In maart 2006 hebben het Europees Parlement en de Raad een richtlijn goedgekeurd betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.

De richtlijn heeft ten doel de voorschriften van de lidstaten met betrekking tot de verplichtingen van de aanbieders van elektronische communicatiediensten op het gebied van de bewaring van gegevens te harmoniseren. Zij heeft ten doel de beschikbaarheid van deze gegevens te waarborgen teneinde strafbare feiten te onderzoeken, op te sporen en te vervolgen.

De richtlijn bepaalt met name:

de te bewaren categorieën gegevens;

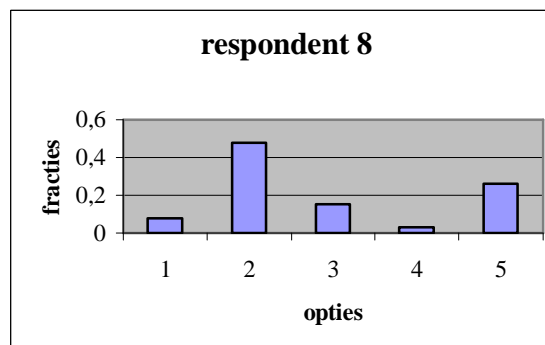
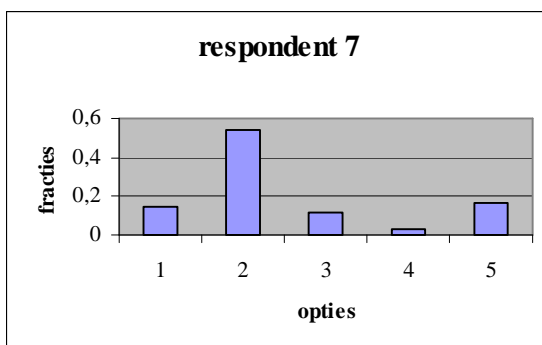
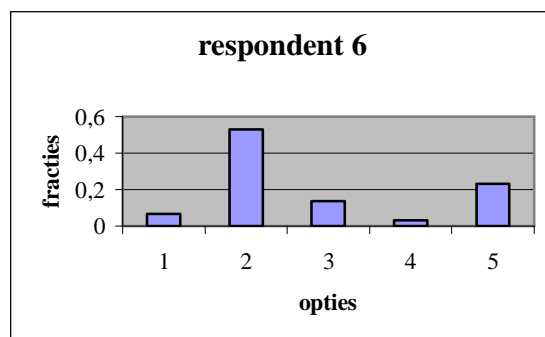
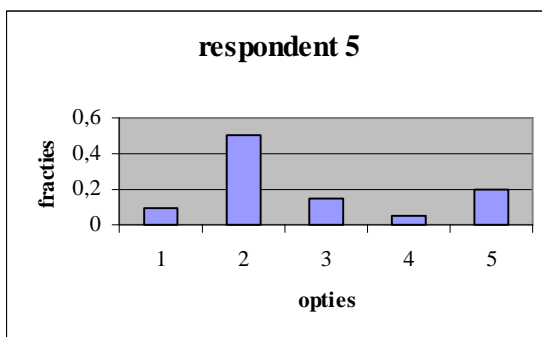
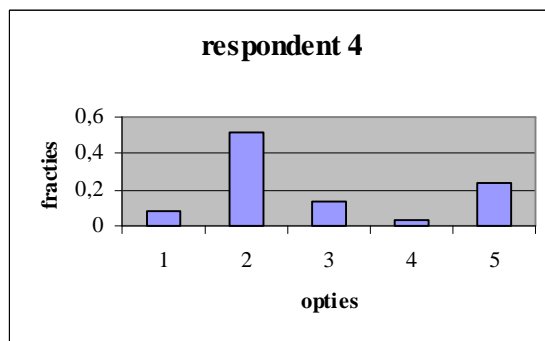
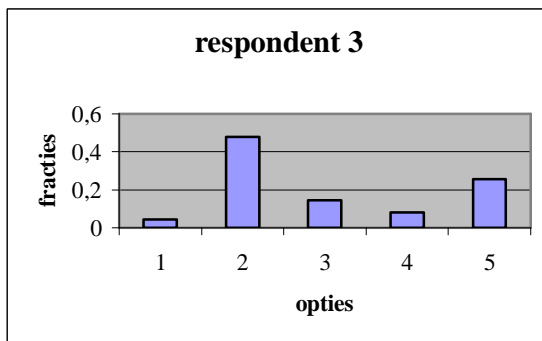
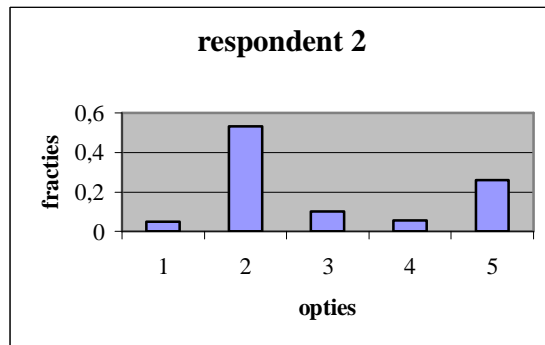
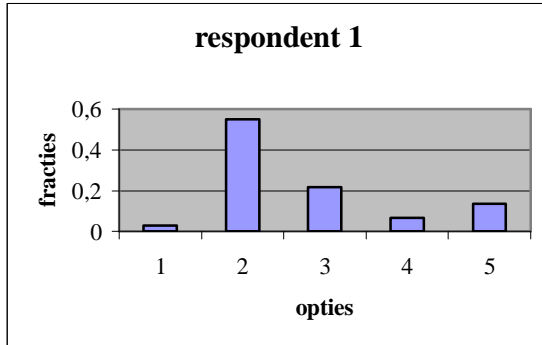
de bewaringstermijnen;

de opslagvoorschriften voor bewaarde gegevens;

de te respecteren beginselen inzake gegevensbeveiliging

## Bijlage 7 Alle histogrammen AHP

De losse histogrammen per respondent met de verschillende voorkeuren per respondent door middel van de AHP methode.



### Bijlage 8 Exacte percentages AHP

De exacte percentages van de verschillende respondenten per variabele en de totale percentages van de variabelen door middel van de AHP methode.

respondent	C1	C2	C3	C4	C5
1	0,03077	0,54918	0,217405	0,067125	0,13552
2	0,048765	0,53027	0,102138	0,058286	0,26054
3	0,04172	0,47571	0,145032	0,080483	0,25705
4	0,077631	0,51305	0,133528	0,035094	0,2407
5	0,093241	0,50129	0,145831	0,056668	0,20297
6	0,069857	0,52765	0,137015	0,031562	0,23392
7	0,140335	0,54546	0,113873	0,031629	0,1687
8	0,07765	0,47842	0,154042	0,02784	0,26205
gemiddelde	0,072496	0,51513	0,143608	0,048586	0,22018

## Bijlage 9 Reflectieverslag Bacheloropdracht

Dit verslag is een kort reflectieverslag dat zal gaan over het professioneel functioneren tijdens de (voorbereiding en) de uitvoering van de opdracht. Ik heb gekozen voor een opdracht bij een bedrijf buiten de Universiteit Twente. Dit heb ik gedaan om eens een kijkje te nemen buiten de universiteit. Maar het zelf verwerven van een opdracht kost veel voorbereidingstijd. Daarom ben ik ook tijdig begonnen met het zoeken van de opdracht. Dit was zo'n 6 weken voor het begin van de opdracht afgerond. Ik heb een opdracht buiten de universiteit gekozen omdat ik niet wist/weet of ik nu de kant van het openbaar bestuur of de kant van het bedrijfsleven op wil gaan. Daarom heb ik een opdracht in het bedrijfsleven gekozen dat toch raakvlak heeft met de bestuurskunde. Denk hierbij aan de wettelijke restricties die door Nederland en Europa zijn opgelegd en aan de (privacy)risico's die de mensen kunnen lopen. Hierbij kan het algemeen belang in het geding komen.

Voordat ik met mijn opdracht begon ben ik eerst een keer bij Selexyz geweest om duidelijkheid te verkrijgen over wat Selexyz, de universiteit en ik precies van de opdracht verwachtten.

Enkele weken daarna ben ik nog een keer bij Selexyz langs geweest om informatie te krijgen met betrekking tot de RFID technologie en over Selexyz zelf. Deze eerste twee gesprekken had ik met mevrouw Zandbergen, mijn begeleider vanuit Selexyz. Dit is halverwege de opdracht, in week 20, veranderd aangezien ze stopte met haar werkzaamheden voor Selexyz. De heer Jan Veninga heeft vanaf toen de begeleiding op zich genomen.

Van hem heb ik vervolgens een rondleiding gehad in de winkel van Selexyz in Almere. In deze winkel is de RFID technologie al een tijd actief. Daar kon ik zien hoe de RFID technologie in de praktijk werkte. Dit was zeer leerzaam en na de tijd kon ik hem nog vragen stellen over zaken die mij nog niet duidelijk waren.

Naast de heer Veninga waren de begeleiders van de Universiteit de heer Schuur en de heer Heerkens.

Van tevoren was afgesproken dat ik de opdracht thuis, en met veel vrijheid, mocht uitvoeren. Deze manier van werken is mij uiteindelijk goed bevallen. Ik kon mijn tijd zelf indelen en kon aan de opdracht werken wanneer mij dat uitkwam. De medewerkers van Selexyz hebben zich nooit met de vorderingen en uitvoering van mijn opdracht bemoeit maar stonden wel altijd klaar als ik vragen had.

Tegenover die vrijheid die ik kreeg stond wel de 'verplichting' om mijn begeleider op de hoogte te houden van de vorderingen van de opdracht. Dit gebeurde dan ook eens in de



tien dagen. Later, rond de zomervakantie, toen de opdracht de eindfase bereikte gebeurde dit iets minder vaak.

Ik had gehoopt om mijn bacheloropdracht in de beginfase van het nieuwe collegejaar af te ronden. De allereerste planning, waarbij de tijdsspanne 10 weken was, is erg optimistisch gebleken achteraf.

Zeker omdat ik niet met één partij (de universiteit) maar met twee partijen (ook Selexyz) te maken had. Van beide partijen kreeg ik feedback ik graag wilde toepassen. Enerzijds wilde ik natuurlijk graag mijn bachelordiploma halen, anderzijds wilde ik het bedrijf waar ik de opdracht voor mocht uitvoeren en die mij alle vrijheid verleenden niet teleurstellen. U begrijpt dat ik daarom eisen en opdrachten van twee partijen moest verwerken. Ik vond dat ik de goedkeuring van twee partijen nodig had.

De uiteindelijke afronding liep daarnaast ook nog enkele weken vertraging op. Dit kwam door mijn enkelblessure die ik heb opgelopen. Hierdoor kon ik niet bij het tweede groenlicht gesprek aanwezig zijn. We hebben daarom besloten dat gesprek enkele weken te verplaatsen totdat ik weer op de been was.

Na afronding van de opdracht kan ik stellen dat ik veel geleerd heb van deze opdracht. Ten eerste het volledig zelfstandig uitvoeren van een onderzoek en het opstellen van een verslag hierover. Dit had ik natuurlijk al wel eens gedaan maar niet in deze omvang. Wat soms frustrerend was is dat ik bepaalde onderzoeksgegevens niet kwalitatief kon maken. Een voorbeeld: de prijs van boeken daalt als gevolg van het gebruik van de RFID technologie, maar met hoeveel daalt de prijs nu precies? Dit soort gegevens wilde ik graag hard maken om dit aan Selexyz en de universiteit te laten zien, maar dit lukte echter niet.

Waar ik ook van geleerd heb is dat de regie van de opdracht volledig in mijn handen lag. Ik moest alles zelf plannen en als ik het nodig vond om een keer met mijn begeleider van de universiteit of van Selexyz te praten dan moest ik dat zelf aangeven en zelf de afspraak regelen. Ook dit heb ik eigenlijk nooit eerder hoeven doen.

Ook werd mij duidelijk dat het niet eenvoudig is om een verslag op te stellen dat voor twee partijen van betekenis kan zijn. De universiteit hecht natuurlijk waarde aan een opdracht die qua (methodologische) opzet past binnen hetgeen ik in de voorgaande jaren hebt geleerd op de universiteit. Selexyz daarentegen geeft daar niet zo veel om. Zij willen vooral een verslag waar ze iets mee kunnen. Het is leuk om een probleem vast te stellen maar veel belangrijker hoe lossen we dat probleem op? Ik heb echter mijn best gedaan de eisen van beide partijen te verwerken en ben van mening dat het verslag voor beide partijen bevredigend is.

Tot slot was het voor mij leerzaam om eens een kijkje buiten de universiteit te nemen. Ik twijfel immers nog steeds wat ik nu precies wil gaan doen na mijn studie en daarom was de keuze om een opdracht buiten de universiteit te doen een goede.

### **Uiteindelijke tijdsindeling bacheloropdracht**

Wk 10   06 maart 2007		Oriëntatiegesprek met docent
-----		
Wk 16   16 april 2007		Start Bacheloronderzoek
Wk 17   23 april 2007	(01)	<i>Oriënteren en onderzoeksopzet maken</i>
-----		
Wk 18   30 april 2007	(02)	Eerste bijeenkomst met docenten
Wk 19   07 mei 2007	(03)	<i>Theoretisch kader vaststellen</i>
Wk 20   14 mei 2007	(04)	-
Wk 21   21 mei 2007	(05)	-
-----		
Wk 22   28 mei 2007	(06)	Tweede bijeenkomst met docenten
Wk 23   04 juni 2007	(07)	<i>Dataverzameling en analyse</i>
Wk 24   11 juni 2007	(08)	-
Wk 25   18 juni 2007	(09)	-
-----		
Wk 26   25 juni 2007	(10)	Derde bijeenkomst met docenten
Wk 27   02 juli 2007	(11)	<i>Conclusies trekken en aanbevelingen doen</i>
-----		
<i>Tm week 32 zomervakantie</i>		
-----		
Wk 32   06 augustus 2007	(16)	Vierde bijeenkomst met docenten (groenlicht gesprek)
Wk 33   13 augustus 2007	(17)	<i>Feedback toepassen</i>
-----		
Wk 34   20 augustus 2007	(18)	Groenlicht gesprek (kon geen doorgang vinden)
Wk 35   27 augustus 2007	(19)	-
-----		
Wk 36   03 september 2007	(20)	Groenlicht gesprek (goedgekeurd)
-----		
Wk 44   29 oktober 2007		Bachelor colloquium

## Bijlage 10 Samenvatting

RFID staat voor Radio Frequency Identification. Het is een techniek die kan identificeren door middel van radiogolven. Hierdoor kan men van een afstand informatie opslaan en lezen van zogenaamde RFID-tags die op of in objecten zitten. RFID-tags zijn RFID chips in combinaties met antennes om zo de gegevens af te lezen.

Ook Selexyz wil van deze theorie gebruik maken. Ze wil RFID tags op haar boeken plaatsen. Op 28 december 2005 is er definitief besloten de nieuwe selexyz boekwinkel in Almere, Selexyz Scheltema, in te richten op basis van RFID-technologie op item level. Ieder boek werd voorzien van een eigen unieke RFID-tag. Vervolgens werd in november 2006 Selexyz Dominicanen in Maastricht geopend. Ook deze winkel is ingericht op de RFID technologie.

De voordelen van deze technologie voor Selexyz zijn onder andere het sneller checken van voorraden en het sneller zoeken van boeken. Daarnaast is er een onderzoek gedaan naar wat consumenten nu precies belangrijke voordelen vinden van de RFID technologie. Deze voordelen zijn door mij opgesteld. De belangrijkste voordelen waren de lagere prijzen voor boeken en het sneller en makkelijker bestellen van ontbrekende boeken.

Maar naast deze voordelen die de RFID technologie voor Selexyz heeft zijn er ook nadelen. Dit zijn met name privacybezwaren die mensen zien. De voornaamste bezwaren zijn het categoriseren en het volgen van mensen en het uitlezen van persoonsgegevens vanaf RFID tags. Hier zijn echter ook veel relativeringen bij te vinden. Zo is het bijvoorbeeld niet mogelijk om tags van meer dan 10 meter afstand uit te lezen. Deze complete opsomming van relativeringen kunt u terugvinden in het verslag.

Tot slot is niet geheel duidelijk wat er nu over het gebruik van de RFID tags in de wetgeving staat. Er is tenslotte de mogelijkheid om persoonsgegevens op te slaan en uit te lezen en de mogelijkheid om personen te volgen en te categoriseren.

We zien dat er veel Europese wetgeving bestaat over de bescherming van de privacy. In Nederland bestaat een dergelijke wetgeving niet en moeten we ons beroepen op de Wet Bescherming Persoonsgegevens.

Aan het einde van het verslag zijn nog wat aanbevelingen van mij te vinden. Zo zou Selexyz de RFID technologie bijvoorbeeld kunnen combineren met een klantenkaart. De klanten die van deze technologie/kaart gebruik willen maken kunnen op voordeel rekenen. Op deze manier zullen de klanten de RFID technologie sneller accepteren.