Kader voor effectbeoordeling op het gebied van de bescherming van de persoonlijke levenssfeer en persoonsgegevens voor RFID-toepassingen

11 februari 2011

INDEX

1. Inleiding

De Europese Commissie (de "Commissie") heeft op 12 mei 2009 een aanbeveling uitgevaardigd over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen ("RFID-aanbeveling"). De Commissie heeft in deze aanbeveling een vereiste opgenomen dat de Groep gegevensbescherming van artikel 29 een door de industrie opgesteld kader voor effectbeoordeling op het gebied van persoonlijke levenssfeer en persoonsgegevens voor RFID-toepassingen moet goedkeuren. Deze beoordelingen worden gewoonlijk "privacyeffectbeoordelingen" (PEB's) genoemd. Dit kader voor PEB's voor RFID-toepassingen ("het kader") behandelt dit vereiste.

Het uitvoeren van PEB's voor RFID-toepassingen biedt tal van voordelen. Zij helpen exploitanten van RFID-toepassingen om:

- procedures ter naleving van wet- en regelgeving voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens op te zetten en te handhaven;
- risico's voor hun organisatie en voor gebruikers van de RFID-toepassing te beheren (met betrekking tot naleving van de bescherming van de persoonlijke levenssfeer en persoonsgegevens en uit het oogpunt van publieke beeldvorming en vertrouwen van de consument); en
- collectieve voordelen van RFID-toepassingen te bieden, waarbij de succesvolle bescherming van de persoonlijke levenssfeer wordt geëvalueerd door ontwerpinspanningen in de vroege stadia van het specificatie- of ontwikkelingsproces.

De PEB-procedure is gebaseerd op een aanpak van risicobeheer voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens die voornamelijk is gericht op de uitvoering van de Europese RFID-aanbeveling. Deze aanpak strookt met het rechtskader en de beste praktijken van de EU.

De PEB-procedure is bedoeld om exploitanten van RFID-toepassingen te helpen bij het blootleggen van risico's voor de persoonlijke levenssfeer van een RFID-toepassing, het beoordelen van de waarschijnlijkheid ervan en het documenteren van de stappen die zijn genomen om deze risico's aan te pakken. Deze (eventuele) effecten zouden aanzienlijk uiteen kunnen lopen, afhankelijk van het feit of de RFID-toepassing al dan niet persoonsgegevens verwerkt. Het PEB-kader biedt exploitanten van RFID-toepassingen richtsnoeren betreffende de risicobeoordelingsmethoden, met inbegrip van passende maatregelen om waarschijnlijke effecten op privacy- en gegevensbescherming op efficiënte, effectieve en evenredige wijze te beperken.

Tot slot is het PEB-kader voldoende algemeen om voor alle RFID-toepassingen te kunnen gelden, terwijl bijzonderheden en specifieke kenmerken op sectoraal niveau of naar gelang van het soort toepassing kunnen worden behandeld.

Het PEB-kader maakt deel uit van de context van andere informatiezekerheids-, gegevensbeheer- en operationele normen die goede instrumenten voor gegevenskwaliteitsbeheer voor RFID- en andere toepassingen aanreiken. Het huidige kader kan als grondslag dienen om industrie-, sector- en/of toepassingsspecifieke PEB-formulieren op te stellen. Zoals voor de uitvoering van elk theoretisch document geldt, vereist het PEB-kader mogelijk een verduidelijking van de toepassing van de termen evenals op praktische ervaring gebaseerde richtsnoeren betreffende praktijken, die tot de uitvoering ervan kunnen bijdragen.

1.1. Hoofdbegrippen

Een aantal begrippen die in het kader worden gebruikt, moeten nader worden omschreven. ***RFID*** is een technologie die gebruikmaakt van elektromagnetische golven om met RFID-tags te communiceren, waarbij het mogelijk is de unieke identificatienummers van de RFID-tags of eventueel andere, daarin opgeslagen informatie te lezen. ***RFID-tags*** zijn doorgaans klein en kunnen verschillende vormen aannemen, maar bestaan meestal uit een elektronisch geheugen, dat leesbaar en eventueel overschrijfbaar is, en antennes. ***RFID-lezers*** worden gebruikt om de informatie in RFID-tags te lezen.

RFID-toepassingen verwerken informatie die door middel van RFID-tags en RFID-lezers tot stand is gebracht. Dergelijke toepassingen worden door een of meer ***exploitanten van RFID-toepassingen*** geëxploiteerd en worden ondersteund door back-endsystemen en communicatienetwerkinfrastructuren. Indien een exploitant van RFID-toepassingen afwegingen maakt met betrekking tot de verzameling of het gebruik van persoonsgegevens, zou zijn rol vergelijkbaar kunnen zijn met die van de voor verwerking verantwoordelijken als bepaald in Richtlijn 95/46/EG. Hij wordt dan omschreven als de natuurlijke of rechtspersoon, overheid, agentschap of elke ander instantie die alleen of gezamenlijk met anderen de doelstellingen en middelen bepaalt voor het exploiteren van een RFID-toepassing die effecten heeft op persoonsgegevens.

In de context van RFID-technologie is de volgende classificatie van toepassing:

- Een ***privacyeffectbeoordeling (PEB)*** is een procedure waarbij op doordachte en systematische wijze getracht wordt de effecten op het gebied van de bescherming van de persoonlijke levenssfeer en persoonsgegevens van een specifieke RFID-toepassing te beoordelen. Het doel hiervan is passende maatregelen te nemen om deze effecten te voorkomen of ten minste te beperken.
- Het ***kader*** bepaalt de doelstellingen van PEB's voor RFID-toepassingen, de componenten van RFID-toepassingen die tijdens PEB's in aanmerking moeten worden genomen en de gemeenschappelijke structuur en inhoud van PEB-verslagen voor RFID-toepassingen.
- Een ***PEB-verslag*** is het document dat uit de PEB-procedure voortvloeit en aan de bevoegde autoriteiten ter beschikking wordt gesteld. Door eigendomsrechten beschermde en veiligheidsgevoelige informatie mag uit PEB-verslagen worden verwijderd voordat de verslagen naar buiten worden gebracht (bv. aan de bevoegde autoriteiten) zolang de informatie niet specifiek betrekking heeft op gevolgen voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens. De wijze waarop de PEB ter beschikking wordt gesteld (bv. al dan niet op verzoek), wordt bepaald door de lidstaten. In het bijzonder kan rekening worden gehouden met het gebruik van speciale gegevenscategorieën, alsook met andere factoren zoals de aanwezigheid van een functionaris voor gegevensbescherming.
- ***PEB-formulieren*** kunnen op basis van het kader worden opgesteld ter verstrekking van op de industrie gebaseerde, op de toepassing gebaseerde of andere specifieke formaten voor PEB's en bijbehorende PEB-verslagen.

Deze en andere termen, zoals ***gebruikers*** **en** ***persoon***, staan voor de toepassing van dit PEB-kader ook beschreven in aanhangsel B: Verklarende woordenlijst. Termen uit Richtlijn 95/46/EG inzake gegevensbescherming zijn er ter verwijzing in opgenomen.

De uitvoering en verslaggeving, in voorkomend geval, van PEB's vormen aanvullende verplichtingen op die welke exploitanten van RFID-toepassingen eventueel volgens bijzondere wet- en regelgeving en andere bindende overeenkomsten moeten nakomen.

1.2. Interne procedures

Exploitanten van RFID-toepassingen moeten beschikken over hun eigen interne procedures ter ondersteuning van de uitvoering van PEB's, zoals:

- *Planning van de PEB-procedure,* zodat er voldoende tijd is om eventuele aanpassingen in de RFID-toepassing aan te brengen en het PEB-verslag minstens zes weken vóór de uitvoering aan de bevoegde autoriteiten beschikbaar te stellen.
- *Interne toetsing van de PEB-procedure (inclusief de initiële analyse) en PEB-verslagen* op consistentie met andere documentatie met betrekking tot de RFID-toepassing, zoals systeemdocumentatie, productdocumentatie en voorbeelden van productverpakkingen en RFID-tagimplementatie. De interne toetsing moet uitwisseling van feedback behelzen om effecten aan te pakken die na de implementatie van de toepassing zijn verzameld en om rekening te houden met resultaten van eerdere PEB's.
- *Samenstelling van ondersteunend materiaal* (dat resultaten van veiligheidscontroles, ontwerpen van controlemechanismen en kopieën van kennisgevingen kan bevatten) ter staving dat de exploitant van RFID-toepassingen aan alle geldende verplichtingen heeft voldaan.
- *Aanwijzing van de personen en/of functies binnen het bedrijf die bevoegd zijn relevante maatregelen te nemen* tijdens de PEB-procedure (bv. het uitvoeren van de initiële PEB-analyse en het opstellen en ondertekenen van het PEB-verslag, het bijhouden van toepasselijke documenten en het scheiden van taken voor deze functies).
- *Verstrekking van criteria voor het evalueren en documenteren of de toepassing al dan niet gereed is voor implementatie* in lijn met het kader en relevante PEB-formulieren.
- *Het in aanmerking nemen/identificeren van factoren die een nieuw of herzien PEB-verslag zouden vereisen* is wenselijk. De criteria moeten betrekking hebben op het volgende: significante wijzigingen in de RFID-toepassing, zoals ingrijpende wijzigingen die verder gaan dan de oorspronkelijke doeleinden (bv. secundaire doeleinden); soorten verwerkte gegevens; gebruik van de informatie dat de gehanteerde controlemechanismen verzwakt; onverwachte inbreuk in verband met persoonsgegevens[1] met een beslissend effect en die niet onder de door de eerste PEB geïdentificeerde resterende risico's van de toepassing viel; bepaling van een regelmatige herzieningsperiode; het reageren op substantiële of significante feedback of informatie van interne of externe belanghebbenden; of significante technologische veranderingen met consequenties voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens voor de desbetreffende RFID-toepassing. Ingrijpende wijzigingen die de reikwijdte van de verzameling of het gebruik beperken, hoeven niet per se tot een herziening van de PEB te leiden. Tijdens de hele levensduur van de RFID-toepassing is een nieuw of herzien PEB-verslag wenselijk indien de RFID-toepassing wordt gewijzigd in de mate zoals beschreven in het hoofdstuk over de initiële analyse.
- *Raadpleging van belanghebbenden.* De meningen en feedback van relevante belanghebbenden met betrekking tot de onderzochte RFID-toepassing moeten worden beschouwd als onderdeel van de PEB-beoordeling van mogelijke problemen en vraagstukken. De raadpleging moet aansluiten op de omvang, reikwijdte, aard en het niveau van de RFID-toepassing. In bedrijven zijn personen belast met de taak toe te zien op privacy binnen het bedrijf of de afdeling. Deze personen vormen

[1] In dit geval geldt de definitie die is vermeld in Richtlijn 2009/136/EG tot wijziging van Richtlijn 2002/58/EG, zie pagina 29 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:NL:PDF.

belangrijke deelnemers aan de PEB-procedure voor zover zij betrokken zijn bij de specifieke RFID-toepassingen of het toezicht erop. Werknemers met kennis van technische, marketing- en andere disciplines kunnen ook noodzakelijke deelnemers van de procedure zijn, afhankelijk van de aard van de RFID-toepassing en de rol die zij daarin spelen. RFID-exploitanten kunnen over raadplegingsmechanismen beschikken, waarbij externe belanghebbenden, zowel personen als organisaties of autoriteiten, met hen kunnen communiceren en feedback kunnen geven. Voor zover van toepassing dient de RFID-exploitant gebruik te maken van raadplegingsmechanismen om informatie te verkrijgen van groepen die personen vertegenwoordigen van wie de persoonlijke levenssfeer rechtstreeks door de voorstellen beïnvloed wordt, bv. werknemers en klanten van de RFID-exploitant.

2. De PEB-procedure

Het kader beoogt exploitanten van RFID-toepassingen richtsnoeren te verstrekken om PEB's voor specifieke RFID-toepassingen uit te voeren, zoals de Commissie in de aanbeveling heeft gevraagd. Voorts dienen de gemeenschappelijke organisatorische structuur en inhoud van de PEB-verslagen te worden vastgesteld, waarin de resultaten van de PEB's moeten worden vastgelegd. Aangezien een groot aantal exploitanten van RFID-toepassingen binnen bepaalde sectoren dezelfde of soortgelijke RFID-toepassingen overwegen, biedt het kader een basis voor de opstelling van PEB-formulieren voor specifieke toepassingen of industriële sectoren. PEB-formulieren kunnen deze sectoren helpen PEB's efficiënter uit te voeren en de bijbehorende verslagen voor deze soortgelijke RFID-toepassingen op te stellen[2]. Aangezien gemeenschappelijke RFID-toepassingen in verschillende lidstaten kunnen worden aangeboden, is het kader bedoeld om vereisten voor exploitanten van RFID-toepassingen volgens lokale wet- en regelgeving, beste praktijken en andere bindende overeenkomsten te harmoniseren.

Het kader behandelt de procedure voor het uitvoeren van PEB's van RFID-toepassingen vóór de implementatie ervan en geeft de werkingssfeer van de bijbehorende PEB-verslagen aan[3].

Exploitanten van RFID-toepassingen moeten een PEB ontwikkelen voor elke RFID-toepassing die zij exploiteren. Indien zij meerdere RFID-toepassingen implementeren (eventueel in dezelfde context of op dezelfde locatie), kunnen zij één PEB-verslag opstellen mits de beperkingen en verschillen van de toepassingen nadrukkelijk in dit verslag worden vermeld. Als exploitanten van RFID-toepassingen één RFID-toepassing op dezelfde manier hergebruiken voor meerdere producten, diensten of processen, mogen zij één PEB-verslag opstellen voor alle producten, diensten of processen die soortgelijk zijn (bijvoorbeeld een autofabrikant die in dezelfde bedrijfsomstandigheden in alle wagens dezelfde antidiefstalmechanismen installeert). De uitvoering en verslaggeving, in voorkomend geval, van PEB's vormen aanvullende verplichtingen op die welke exploitanten van RFID-toepassingen eventueel volgens specifieke toepasselijke wet- en regelgeving en andere bindende overeenkomsten moeten nakomen.

De PEB-procedure bestaat uit twee fasen:

---

2 Onderlinge of meervoudige erkenning in verschillende entiteiten en sectoren voor de implementatie van eerder gekeurde RFID-toepassingen moet worden onderzocht.

3 Punt 5 (a) van de aanbeveling van de Europese Commissie van mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen C(2009) 3200 definitief.

1. **Fase van initiële analyse**: de exploitant van RFID-toepassingen moet de in dit hoofdstuk beschreven stappen volgen om te bepalen:

   a) of een PEB van zijn RFID-toepassing al dan niet is vereist; en

   b) of een PEB op grote schaal of op kleine schaal wenselijk is.

2. **Fase van risicobeoordeling**: hierin worden de criteria en aspecten van PEB's op grote schaal en op kleine schaal uiteengezet.

2.1. Fase van initiële analyse

Om een PEB voor een specifieke toepassing te kunnen uitvoeren, moeten bedrijven in de eerste plaats begrijpen hoe een dergelijke procedure in de praktijk moet worden gebracht uitgaande van de aard en gevoeligheid van de gegevens, de aard en soort van verwerking of beheer van de informatie en de soort RFID-toepassing in kwestie. Bedrijven die reeds beschikken over procedures voor beoordeling van privacyrisico's voor andere toepassingen kunnen gebruikmaken van de classificatiecriteria en procedurestadia om hun bestaande PEB-procedures af te stemmen op dit kader.

Voor de initiële beoordeling moeten exploitanten van RFID-toepassingen de besluitvormingsstructuur in figuur 1 doorlopen. Zo kan de RFID-exploitant bepalen of en in welke mate een PEB voor de desbetreffende RFID-toepassing is vereist.

Het bijbehorende niveau in de initiële fase helpt te bepalen hoe gedetailleerd de risicobeoordeling moet zijn (bv. een PEB op grote schaal of op kleine schaal).

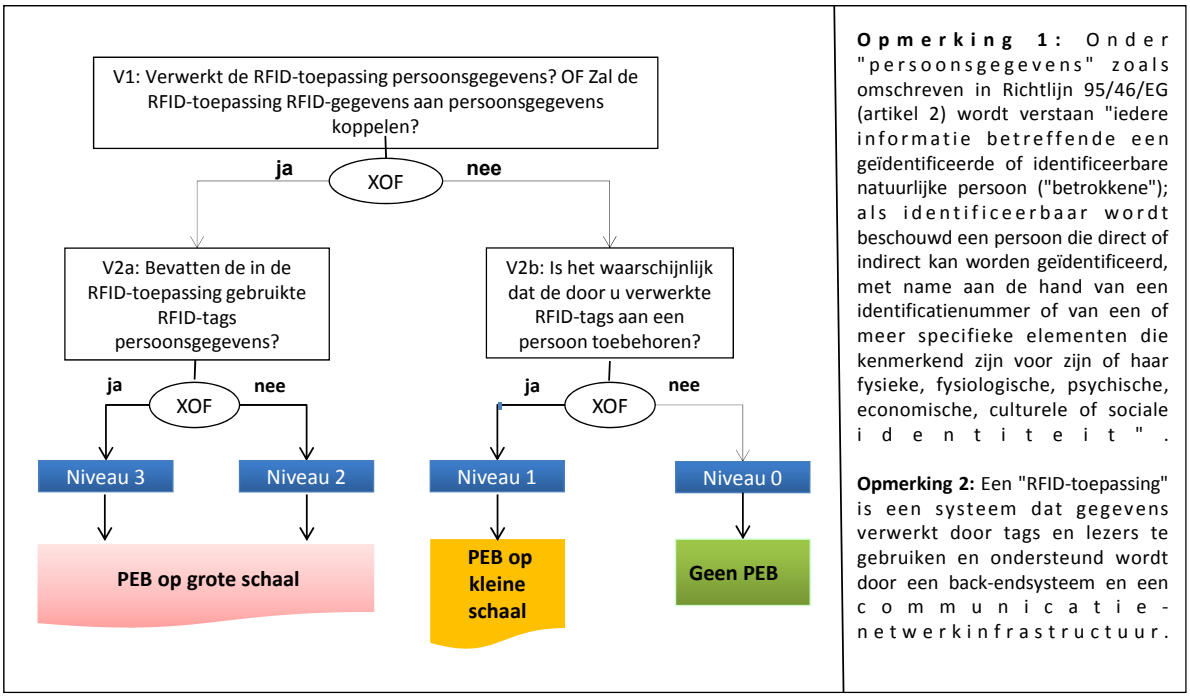
Deze initiële analyse moet worden gedocumenteerd en desgewenst aan gegevensbeschermingsinstanties ter beschikking worden gesteld. Zie bijlage I voor documentatierichtsnoeren.

PEB op grote schaal

Een PEB op grote schaal is vereist voor toepassingen die in de fase van initiële analyse in hoofdstuk 2.1 onder niveau 2 of niveau 3 worden ingedeeld. Voorbeelden van toepassingen waarvoor een PEB op grote schaal nodig is, zijn toepassingen die persoonsgegevens verwerken (niveau 2) of waarbij de RFID-tag persoonsgegevens bevat (niveau 3). Hoewel zowel niveau 2 als niveau 3 tot een PEB op grote schaal leiden, identificeren zij verschillende risico-omgevingen en bieden zij daarom verschillende risicobeperkingsstrategieën. Toepassingen van niveau 2 kunnen bijvoorbeeld over controlemechanismen beschikken ter bescherming van back-endgegevens, terwijl toepassingen van niveau 3 over controlemechanismen beschikken die zowel back-endgegevens als taggegevens beschermen. Het bedrijfsleven kan deze niveaus en de wijze waarop zij de PEB-procedure beïnvloeden, op grond van verdere ervaring meer verfijnen. Als de toepassing persoonsgegevens verwerkt, is een zeer gedetailleerde risicobeoordeling (op grote schaal) nodig om ervoor te zorgen dat risicobeperkende maatregelen goed worden uitgewerkt. Dit helpt de exploitant van RFID-toepassingen bij het vaststellen van relevante risico's en het ontwikkelen van geschikte controlemechanismen. In deze context moeten exploitanten ook in ogenschouw nemen of de informatie van de RFID-tag nog voor andere doeleinden gebruikt zal worden dan de initiële doeleinden of context zoals door de persoon is begrepen. Dit is met name het geval als de informatie gebruikt kan worden om persoonsgegevens te verwerken of eraan te koppelen. Exploitanten moeten ook nagaan of een nieuwe PEB-analyse wenselijk is en of andere controlemechanismen voor risicobeperking moeten worden toegepast.

PEB op kleine schaal

PEB's op kleine schaal volgen dezelfde procedure als PEB's op grote schaal, maar gezien het lagere risicoprofiel is een PEB op kleine schaal beperkter qua toepassingsgebied en gedetailleerdheid wat betreft het onderzoek en het verslag dan een PEB op grote schaal. PEB's op kleine schaal zijn bedoeld voor toepassingen van niveau 1. Hoewel een PEB op kleine schaal een soortgelijke procedure als een PEB op grote schaal volgt, zijn de vereiste controlemechanismen en bijbehorende documentatie in het PEB-verslag vereenvoudigd, aangezien de relevante risico's van een toepassing van niveau 1 lager zijn dan niveau 2 of niveau 3.



Figuur 1: Besluitvormingsstructuur ter bepaling of en hoe gedetailleerd een PEB moet worden uitgevoerd

2.2. Fase van risicobeoordeling

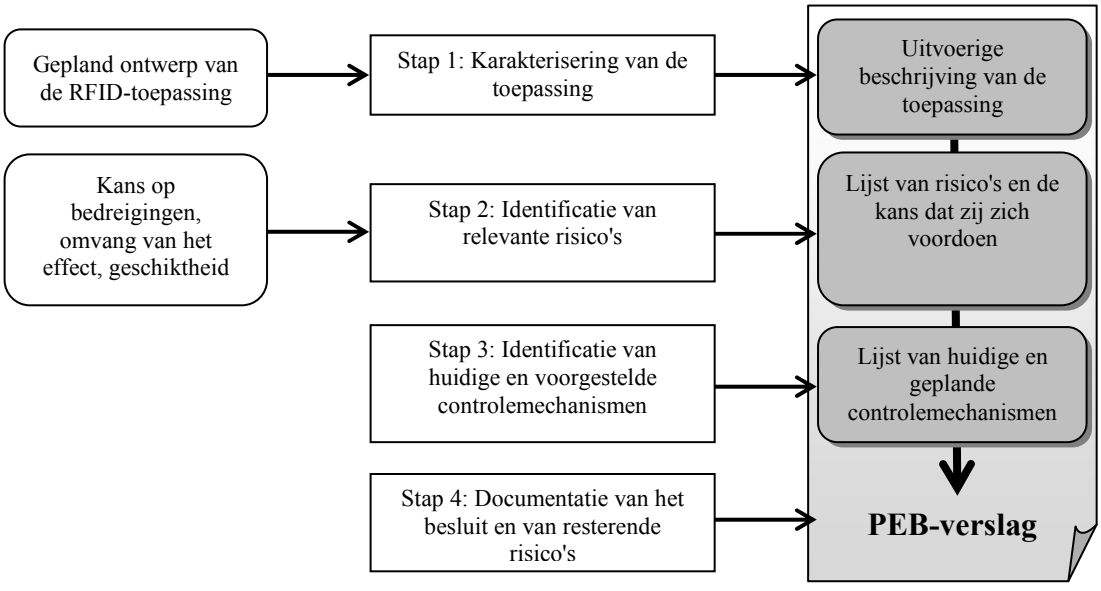
Een risicobeoordeling heeft ten doel de risico's voor de persoonlijke levenssfeer van een RFID-toepassing vast te stellen, bij voorkeur in een vroeg stadium van systeemontwikkeling, en te documenteren hoe deze risico's *op proactieve wijze* beperkt worden door technische en organisatorische controlemechanismen. Op deze manier spelen PEB's een belangrijke rol in de naleving en de wettelijke vereisten inzake privacy (Richtlijn 95/46) en vormen zij een maatregel waarmee de effectiviteit van risicobeperkingsprocedures wordt beoordeeld. Om tijd en kosten te besparen, is het raadzaam deze fase van risicobeoordeling geruime tijd voordat definitieve beslissingen over de architectuur van een RFID-toepassing worden gemaakt, te doorlopen. Zo kunnen technische strategieën voor beperking van risico's voor de persoonlijke levenssfeer in het ontwerp van het systeem worden meegenomen in plaats van dat er achteraf nog aan moet worden gesleuteld.

Tijdens een risicobeoordelingsprocedure wordt standaard in eerste instantie gekeken met welke waarschijnlijkheid een RFID-toepassing risico's meebrengt en hoe groot de gevolgen ervan zijn. Het wordt exploitanten van RFID-toepassingen aangeraden als uitgangspunt voor hun risicobeoordeling de doelstellingen inzake de persoonlijke levenssfeer van de EU-

richtlijn te gebruiken (zie bijlage II). De risico's voor de persoonlijke levenssfeer kunnen groot zijn, omdat zich bij de implementatie van de RFID-toepassing kwaadaardige aanvallen kunnen voordoen of omdat er vanuit de organisatie of de omgeving geen controlemechanismen voor de persoonlijke levenssfeer bestaan. De risico's voor de persoonlijke levenssfeer kunnen ook klein zijn, simpelweg omdat het onwaarschijnlijk is dat zij zich in de desbetreffende omgeving of organisatie voordoen, of omdat de RFID-toepassing al op een manier is geconfigureerd die uitermate veilig is voor de persoonlijke levenssfeer. Tijdens de PEB-procedure wordt getracht alle potentiële risico's in aanmerking te nemen waarna de omvang, kans dat ze zich voordoen en mogelijke beperkingsmaatregelen worden bestudeerd. Dit leidt tot de identificatie van risico's voor de persoonlijke levenssfeer die echt van belang zijn voor de implementatie van de RFID-toepassing van het bedrijf en die door middel van effectieve controlemechanismen moeten worden beperkt.

Tijdens de PEB-procedure (zoals weergegeven in figuur 2) hebben exploitanten van RFID-toepassingen de volgende taken:

1. Beschrijving van de RFID-toepassing;
2. Identificatie en opsomming van de wijze waarop de RFID-toepassing de persoonlijke levenssfeer kan bedreigen en schatting van de omvang en waarschijnlijkheid van die risico's;
3. Documentatie van de bestaande en voorgenomen technische en organisatorische controlemechanismen ter beperking van de geïdentificeerde risico's; en
4. Documentatie van het besluit (resultaten van de analyse) met betrekking tot de toepassing.



Stap 1: Karakterisering van de toepassing

De karakterisering van de toepassing moet een uitgebreid en volledig beeld geven van de toepassing, de omgeving en systeemgrenzen ervan. Het ontwerp van de toepassing, de bijbehorende interfaces met andere systemen en informatiestromen worden hierin beschreven. Gegevensstroomdiagrammen die de verwerking van primaire en secundaire gegevens laten zien, worden aanbevolen zodat informatiestromen kunnen worden weergegeven. Ook gegevensstructuren moeten worden gedocumenteerd, zodat mogelijke koppelingen kunnen worden geanalyseerd. In bijlage I worden de elementen samengevat die een RFID-toepassing karakteriseren met het oog op een PEB.

Daarnaast wordt ook informatie met betrekking tot de operationele en strategische omgeving van de toepassing aanbevolen. Deze informatie bestaat uit de onmiddellijke en langetermijntaken van het systeem, belanghebbenden op het gebied van gegevensverzameling, functionele vereisten, alle potentiële gebruikers en een beschrijving van de architectuur en gegevensstromen van de RFID-toepassing (met name interfaces naar externe systemen die persoonsgegevens kunnen verwerken).

Stap 2: Identificatie van de risico's

Deze stap beoogt omstandigheden te identificeren die persoonsgegevens kunnen bedreigen of in gevaar kunnen brengen. Hierbij wordt gebruikgemaakt van de EU-richtlijn als leidraad voor belangrijke kenmerken van te beschermen doelstellingen inzake de persoonlijke levenssfeer. Er kunnen risico's verbonden zijn aan de componenten van RFID-toepassingen, de functies ervan (verzameling, opslag en verwerking) en de omgeving van gegevensuitwisseling en -verwerking waarin zij zijn ingebed.

In bijlage III is een lijst van potentiële risico's voor de persoonlijke levenssfeer opgenomen. Deze lijst fungeert als leidraad voor de systematische identificatie van potentiële risico's die de doelstellingen van de EU-richtlijn (bijlage II) bedreigen.

Naast de identificatie van de risico's moeten PEB's deze risico's ook dienovereenkomstig kwantificeren. Exploitanten van RFID-toepassingen moeten, op grond van het evenredigheidsbeginsel en volgens redelijke voorwaarden, rekening houden met de *waarschijnlijkheid* van risico's voor de persoonlijke levenssfeer. Risico's kunnen zich in en, waar mogelijk, buiten de specifieke RFID-toepassing voordoen. Deze risico's kunnen worden afgeleid van zowel het waarschijnlijke gebruik als het mogelijke misbruik van de informatie, en met name als de in de RFID-toepassing gebruikte RFID-tags operationeel blijven nadat zij in het bezit van personen zijn gekomen**.**

Tijdens de risicobeoordeling moeten de desbetreffende risico's met oog voor de persoonlijke levenssfeer worden geëvalueerd; RFID-exploitanten moeten rekening houden met:

1. De significantie van een risico en de kans dat het zich voordoet.
2. De omvang van het effect als het risico zich zou voordoen.

Het bijbehorende risiconiveau kan vervolgens worden geclassificeerd als laag, matig of hoog.

Een risico dat een belangrijk voorwerp van discussie is, is dat RFID-tags kunnen worden gebruikt voor het opstellen van een profiel en/of voor het volgen van personen. In dat geval zou de informatie van de RFID-tag, met name de identificatiecode(s), gebruikt worden om

een bepaalde persoon opnieuw te identificeren. Kleinhandelaren die RFID-tags doorverkopen aan klanten zonder deze automatisch te deactiveren of te verwijderen aan de kassa *kunnen* dit risico onbedoeld in werking stellen. Een belangrijke vraag hierbij is echter of dit risico waarschijnlijk is en daadwerkelijk de vorm van een *ontoelaatbaar* risico aanneemt of niet. Volgens punt 11 van de RFID-aanbeveling dienen kleinhandelaren op de plaats van verkoop tags die gebruikt worden in hun toepassing te deactiveren of te verwijderen tenzij consumenten, nadat zij op de hoogte zijn gebracht van het beleid overeenkomstig dit kader, hun toestemming hebben verleend om de tags operationeel te houden. Kleinhandelaren hoeven tags niet te deactiveren of te verwijderen indien in het PEB-verslag wordt vastgesteld dat tags die in kleinhandeltoepassingen worden gebruikt en operationeel blijven na de verkoop, geen waarschijnlijke bedreiging vormen voor de persoonlijke levenssfeer of de bescherming van persoonsgegevens, als bepaald in punt 12 van de aanbeveling. Onder deactivering van tags wordt verstaan elk proces dat de interactie van een tag met zijn omgeving stopt waarvoor geen actieve betrokkenheid van de consument nodig is.

Sectorspecifieke formulieren die in de loop der tijd op basis van dit kader zullen worden opgesteld en in verschillende sectoren zullen worden gebruikt, kunnen nauwkeurigere informatie over de identificatie van risico's verstrekken.

Stap 3: Identificatie en aanbeveling van controlemechanismen

Deze stap is bedoeld om de controlemechanismen te analyseren die zijn ingevoerd of zullen worden ingevoerd, teneinde de geïdentificeerde risico's voor de persoonlijke levenssfeer te minimaliseren, te beperken of weg te nemen.

De controlemechanismen kunnen technisch of niet-technisch van aard zijn. Technische controlemechanismen zijn in de toepassing ingebouwd op grond van architecturale keuzes of technisch uit te voeren beleidsregels, bv. standaardinstellingen, authenticatiemechanismen en versleutelingsmethoden. Niet-technische controlemechanismen daarentegen zijn beheer- en operationele mechanismen, bv. operationele procedures. Controlemechanismen kunnen worden aangemerkt als gericht op preventie dan wel op opsporing. De eerstgenoemde beletten pogingen tot schending en de laatstgenoemde mechanismen melden schendingen of pogingen tot schending.

Er kan ook sprake zijn van "van nature aanwezige" controlemechanismen die door de omgeving tot stand zijn gebracht. Als bijvoorbeeld geen lezers zijn geïnstalleerd die artikelen of personen kunnen volgen (d.w.z. omdat er geen zakelijke argumenten voor bestaan), is er van nature ook geen (waarschijnlijk) risico.

De geïdentificeerde risico's en de bijbehorende risiconiveaus moeten helpen bij het bepalen van de relevante geïdentificeerde controlemechanismen die dus moeten worden geïmplementeerd. In de PEB-documentatie moet worden toegelicht hoe de controlemechanismen betrekking hebben op specifieke risico's en hoe de beperking ervan zal leiden tot een aanvaardbaar risiconiveau.

Voorbeelden van controlemechanismen zijn te vinden in bijlage IV.

Stap 4: Documentatie van het besluit en van resterende risico's

Nadat de risicobeoordeling is uitgevoerd, moet het eindbesluit over de toepassing worden vastgelegd in het PEB-verslag, samen met eventuele andere opmerkingen over risico's, controlemechanismen en resterende risico's.

- Een RFID-toepassing wordt goedgekeurd bevonden, nadat volgens de PEB-procedure relevante risico's zijn geïdentificeerd en naar behoren beperkt om ervoor te zorgen dat er geen significante risico's overblijven, om te voldoen aan de nalevingseisen, inclusief relevante interne herzieningen en goedkeuringen.

- Indien een RFID-toepassing in de huidige staat niet goedgekeurd wordt bevonden, moet een specifiek corrigerend actieplan worden opgesteld en een nieuwe privacyeffectbeoordeling worden uitgevoerd om te bepalen of de toepassing een goed te keuren staat heeft bereikt.

In het besluit moeten de volgende gegevens zijn opgenomen:

- Naam van de persoon die het besluit ondertekent.
- Titel van de persoon.
- Datum van het besluit.

PEB-verslag

PEB's zijn interne procedures die gevoelige informatie bevatten die gevolgen kan hebben voor de veiligheid. Daarnaast bevatten zij mogelijk vertrouwelijke en door eigendomsrechten beschermde informatie van het bedrijf met betrekking tot producten en procedures. In dat opzicht moet een PEB-verslag standaard het volgende bevatten:

1. De beschrijving van de RFID-toepassing zoals in bijlage I is vermeld.

2. Documentatie van de vier stappen die hierboven zijn beschreven.

Het ondertekende PEB-verslag, dat een goedgekeurd besluit bevat, moet overeenkomstig de interne procedures van de exploitant van RFID-toepassingen aan de voor gegevensprivacy/-veiligheid aangestelde medewerker van het bedrijf worden bezorgd. Dit verslag wordt verstrekt onverminderd de verplichtingen die in Richtlijn 95/46/EG ten behoeve van voor de verwerking verantwoordelijken zijn vastgesteld, met name de onafhankelijke verplichting tot aanmelding bij de bevoegde autoriteit, als beschreven in afdeling IX van richtlijn 95/46/EG.

3. Slotbepaling

Het PEB-kader treedt in werking uiterlijk zes maanden na publicatie en goedkeuring door de Groep gegevensbescherming artikel 29. Wat betreft RFID-toepassingen die zijn ingevoerd voordat het PEB-kader in werking treedt, is het kader uitsluitend van toepassing wanneer aan de voorwaarden voor de documentatie van een nieuwe of herziene PEB overeenkomstig het PEB-kader is voldaan.

BIJLAGE I - *Karakterisering van de RFID-toepassing*

Exploitanten van RFID-toepassingen moeten onderstaande informatie, voor zover van toepassing, in het PEB-verslag opnemen.

Exploitant van RFID-toepassingen	• Naam en plaats van de rechtspersoon • Persoon of kantoor verantwoordelijk voor de punctualiteit van de PEB • Aanspreekpunt(en) en wijze van informatieaanvraag
Gegevensoverzicht van de RFID-toepassing	• Naam van de RFID-toepassing • Doel(en) van de RFID-toepassing(en) • Basisgebruiksscenario's van de RFID-toepassing • Componenten van de RFID-toepassing en de gebruikte technologie (d.w.z. frequenties, enz.) • Geografisch toepassingsgebied van de RFID-toepassing • Soorten gebruikers/personen op wie de RFID-toepassing betrekking heeft • Individuele toegang en controle
Nummer van het PEB-verslag	• Versienummer van het PEB-verslag (ter onderscheiding van een nieuwe PEB of slechts kleine veranderingen) • Datum van de laatste wijziging in het PEB-verslag
RFID-gegevensverwerking	• Lijst van soorten verwerkte gegevens • Aanwezigheid van gevoelige informatie in de verwerkte gegevens, bv. gezondheidsgegevens
RFID-gegevensopslag	• Lijst van soorten opgeslagen gegevens • Opslagtermijn
Interne RFID-gegevensoverdracht (indien van toepassing)	• Beschrijving of diagrammen van gegevensstromen van interne transacties die van RFID-gegevens gebruikmaken • Doel(en) van de overdracht van persoonsgegevens
Externe RFID-gegevensoverdracht (indien van toepassing)	• Soorten gegevensontvanger(s) • Doel(en) van de overdracht of toegang in het algemeen • Geïdentificeerde en/of identificeerbare (mate van) persoonsgegevens gebruikt bij de overdracht • Overdracht buiten de Europese Economische Ruimte (EER)

BIJLAGE II - *Doelstellingen inzake de persoonlijke levenssfeer*

Momenteel zijn negen doelstellingen inzake de persoonlijke levenssfeer in Richtlijn 95/46/EG vervat. Tijdens de ontwikkeling van de PEB-procedure zijn deze doelstellingen en de bijbehorende RFID-risico's in aanmerking genomen. Deze doelstellingen inzake de persoonlijke levenssfeer zijn in deze bijlage samengevat. Hoewel alle doelstellingen een essentiële rol spelen bij naleving op organisatorisch vlak, is in veel gevallen in de desbetreffende RFID-toepassing alleen een subklasse van deze vereisten aan de orde. De functie van deze doelstellingen is dus om informatie te verstrekken over het ontwerp en de ontwikkeling van de PEB-procedure eerder dan over de uitvoering van bepaalde PEB's.

Beschrijving van de doelstellingen inzake de persoonlijke levenssfeer (gebaseerd op de respectieve EU-privacyrichtlijn(en); hier Richtlijn 95/46/EG)	
Het waarborgen van de kwaliteit van persoonsgegevens	Vermijding en beperking van gegevensgebruik, specificatie en beperking van de doelen, gegevenskwaliteit en transparantie zijn de voornaamste doelstellingen.
Rechtmatigheid van de verwerking van persoonsgegevens	Er moet worden toegezien op de rechtmatigheid van de verwerking van persoonsgegevens door gegevensverwerking te baseren op toestemming, een contract, wettelijke verplichting, enz.
Rechtmatigheid van de verwerking van *gevoelige* persoonsgegevens	Er moet worden toegezien op de rechtmatigheid van de verwerking van gevoelige persoonsgegevens door gegevensverwerking te baseren op nadrukkelijke toestemming, een specifieke wettelijke grondslag, enz.
Naleving van het recht van de betrokkene om te worden ingelicht	Er moet op worden toegezien dat de betrokkene tijdig wordt ingelicht over de verzameling van zijn/haar gegevens.
Naleving van het recht van de betrokkene op gegevenstoegang, gegevensaanpassing en -verwijdering	Er moet tijdig voldaan worden aan de wens van de betrokkene om zijn/haar gegevens te bekijken, aan te passen, te verwijderen of te blokkeren.
Naleving van het recht op bezwaar van de betrokkene	De gegevens van de betrokkene mogen niet langer worden verwerkt indien hij of zij bezwaar maakt. Er moet met name worden toegezien op de transparantie van geautomatiseerde besluiten ten opzichte van personen.
Het waarborgen van een vertrouwelijke en veilige verwerking	Voorkoming van onbevoegde toegang, vastlegging van gegevensverwerking, netwerk- en transportveiligheid en voorkoming van onopzettelijk gegevensverlies zijn de voornaamste doelstellingen.
Naleving van kennisgevingseisen	Kennisgeving over gegevensverwerking, voorafgaande nalevingscontrole en documentatie zijn de voornaamste doelstellingen.
Naleving van gegevensbewaringseisen	Gegevens moeten worden bewaard zolang er reden voor bestaat of zoals wettelijk vereist.

BIJLAGE III - *Risico's voor de persoonlijke levenssfeer*

Deze bijlage bevat een lijst van mogelijke risico's voor de persoonlijke levenssfeer met betrekking tot het gebruik van de RFID-toepassing in kwestie. Het is raadzaam om, met name voor PEB's op grote schaal, risico's systematisch te identificeren met behulp van standaardprocedures voor risicobeoordeling waarin bedreigingen en kwetsbaarheden van een RFID-toepassing aan bod komen.

Onderstaande tabel bevat voorbeelden van risico's die van invloed kunnen zijn op het vermogen van een entiteit om aan de doelstellingen inzake de persoonlijke levenssfeer in bijlage II te voldoen. Exploitanten van RFID-toepassingen kunnen deze lijst gebruiken als uitgangspunt; niet alle risico's zijn echter van toepassing op elke RFID-toepassing. RFID-exploitanten moeten erop toezien dat elk geïdentificeerd risico naar behoren wordt beperkt door een of meer controlemechanismen rekening houdend met de kans dat het risico zich voordoet en de omvang van het effect ervan. Exploitanten van RFID-toepassingen moeten eventueel controlemechanismen bundelen of de bestaande controlemechanismen uitbreiden op basis van factoren zoals de gebruikte technologie, de aard van de implementatie, de soort informatie en de geldende beleidsregels.

Risico voor de persoonlijke levenssfeer	**Beschrijving en voorbeeld**
Niet-gespecificeerd en onbeperkt doel	Het doel van de gegevensverzameling is niet gespecificeerd en gedocumenteerd, of er worden meer gegevens gebruikt dan voor het aangeduide doel is vereist. Voorbeeld: geen documentatie van de doelen waarvoor de RFID-gegevens worden gebruikt en/of gebruik van de RFID-gegevens voor allerlei mogelijke analyses.
Overschrijding van het doel van gegevensverzameling	De gegevens worden verzameld op een identificeerbare wijze die verder gaat dan wat in het doel is aangegeven. Voorbeeld: RFID-betaalkaartgegevens worden niet alleen gebruikt voor de verwerking van transacties, maar ook voor het opstellen van individuele profielen.
Onvolledige informatie of gebrek aan transparantie	De informatie die aan de betrokkene wordt verstrekt over het doel en gebruik van de gegevens is niet volledig, de gegevensverwerking is niet transparant of de informatie wordt niet tijdig verstrekt. Voorbeeld: RFID-informatie aan klanten waarin duidelijke informatie ontbreekt over de wijze waarop RFID-gegevens worden verwerkt en gebruikt, over de identiteit van de exploitant of de gebruikersrechten.

Overschrijding van gegevenskoppeling	Persoonsgegevens worden gekoppeld in een mate die niet vereist is voor het aangeduide doel. Voorbeeld: RFID-betaalkaartgegevens worden gekoppeld aan persoonsgegevens die van een derde zijn verkregen.
Ontbrekende regels of mechanismen voor gegevenswissing	Gegevens worden langer bewaard dan nodig voor het aangeduide doel. Voorbeeld: persoonsgegevens worden verzameld als onderdeel van de toepassing en langer bewaard dan wettelijk toegestaan.
Ongeldigheid van nadrukkelijke toestemming	Toestemming is verkregen met bedreiging van benadeling. Voorbeeld: het is niet mogelijk om wettelijke garanties te gebruiken voor producten of om producten te retourneren/te ruilen als de RFID-tag wordt gedeactiveerd of verwijderd.
Heimelijke gegevensverzameling door de RFID-exploitant	Sommige gegevens worden heimelijk, dus zonder medeweten van de betrokkene, geregistreerd, bv. bewegingsprofielen. Voorbeeld: consumenteninformatie wordt gelezen terwijl klanten voor winkels langslopen of in winkelcentra rondlopen zonder dat zij door een logo of symbool worden ingelicht over de RFID-uitlezingen.
Geen verlening van toegang	De betrokkene kan op geen enkele wijze zijn/haar gegevens aanpassen of wissen. Voorbeeld: een werkgever kan zijn werknemer geen volledig beeld geven van de gegevens die over hem/haar worden bewaard op basis van RFID-toegangs- en -productiegegevens.
Het voorkomen van bezwaren	Er bestaan geen technische of operationele middelen om te kunnen voldoen aan het bezwaar van een betrokkene. Voorbeeld: een ziekenhuisbezoeker kan niet afzien van het uitlezen van gevoelige persoonsgegevens op tags (bv. medicijnen).
Gebrekkige transparantie van geautomatiseerde individuele besluiten	Geautomatiseerde individuele besluiten op basis van persoonlijke aspecten worden toegepast, maar de betrokkenen worden niet ingelicht over de logica van de besluitvorming. Voorbeeld: RFID-exploitanten lezen, zonder klanten hierover in te lichten, alle tags die aan een persoon behoren, inclusief door een andere entiteit verstrekte tags, en bepalen wat voor marketingboodschap de persoon op basis van de tags moet ontvangen.
Ontoereikend beheer van	Toegangsrechten worden niet ingetrokken als ze

toegangsrechten	niet meer nodig zijn. Voorbeeld: met behulp van een RFID-kaart kan een oud-stagiair toegang krijgen tot delen van een bedrijf waar hij/zij niet hoort te zijn.
Ontoereikend authenticatiemechanisme	Een verdacht aantal pogingen tot identificatie en authenticatie wordt niet verhinderd. Voorbeeld: persoonsgegevens op tags worden niet standaard beschermd door een wachtwoord of een ander authenticatiemechanisme.
Onrechtmatige gegevensverwerking	Verwerking van persoonsgegevens wordt niet gebaseerd op toestemming, een contract, wettelijke verplichting, enz. Voorbeeld: een RFID-exploitant deelt verzamelde gegevens met een derde zonder kennisgeving of toestemming zoals anderszins wettelijk bepaald.
Ontoereikend vastleggingsmechanisme	Het ingevoerde vastleggingsmechanisme is ontoereikend. Het legt geen administratieve processen vast. Voorbeeld: er wordt niet vastgelegd wie toegang heeft gehad tot de gegevens van de RFID-werknemerskaart.
Oncontroleerbare vergaring van gegevens vanaf RFID-tags	RFID-tags kunnen worden gebruikt voor het regelmatig opstellen van een profiel en/of volgen van personen. Voorbeeld: kleinhandelaren lezen alle tags die zij kunnen zien.

BIJLAGE IV – *Lijst van voorbeelden van controlemechanismen en beperkende maatregelen voor RFID-toepassingen*

Deze bijlage bevat een lijst van voorbeelden van mogelijke controlemechanismen die exploitanten van RFID-toepassingen kunnen helpen bij het identificeren van geschikte beperkende strategieën. Risico's die tijdens stap twee van de PEB-risicoprocedure als relevant zijn aangemerkt voor de exploitant van RFID-toepassingen, kunnen door middel van een of meer strategieën worden beperkt. Enkele hiervan zijn in deze bijlage beschreven. Het doel van het doorlopen van een PEB-procedure is dat de exploitant van RFID-toepassingen de controlemechanismen identificeert en invoert die nodig zijn om de desbetreffende risico's voor de persoonlijke levenssfeer te beperken.

Mogelijke controlemechanismen zijn:

- Beheerpraktijken voor RFID-toepassingen.
- Individuele toegang en controle.
- Maatregelen voor systeembescherming (waaronder veiligheidscontrolemechanismen).
- Tagbescherming.
- Verantwoordingsmaatregelen.

Deze praktijken vormen een aanvulling op het bestaande regelgevende kader voor gegevensbescherming van de Europese Unie en zijn niet bedoeld ter vervanging hiervan of ter wijziging van de toepassingssfeer ervan.

Beheerpraktijken voor RFID-toepassingen

Beheerpraktijken kunnen het volgende omvatten:

- Managementpraktijken door de exploitant van RFID-toepassingen.
- Verwijdering van RFID-gegevens en beleidslijnen voor wissing ervan.
- Beleidslijnen met betrekking tot rechtmatige verwerking van persoonsgegevens.
- Bepalingen voor gegevensbeperking bij de verwerking van RFID-gegevens, waar mogelijk.
- Verwerking of opslag van gegevens afkomstig van tags die niet aan de RFID-exploitant toebehoren.
- Veiligheidsbeheerpraktijken.

Verstrekking van individuele toegang en controle

- Verstrekking van informatie over de verwerkingsdoelen en de gebruikte categorieën persoonsgegevens.

- Beschrijving van de manier waarop bezwaar gemaakt kan worden tegen de verwerking van persoonsgegevens of hoe de toestemming kan worden ingetrokken.

- Identificatie van de procedure van verzoek om rectificatie of wissing van onvolledige of onnauwkeurige persoonsgegevens.

Systeembescherming

Systeembescherming met betrekking tot passende bescherming van de persoonlijke levenssfeer en persoonsgegevens moet ook in dit deel van het PEB-verslag worden gedocumenteerd. Concepten van systeembescherming zijn van toepassing op back-endsystemen en communicatie-infrastructuur voor zover zij relevant zijn voor de RFID-toepassing. Wanneer zulke concepten van toepassing zijn, dient erkend te worden dat back-endsystemen vaak complex zijn en eventueel een eigen PEB hebben ondergaan. Die analyse moet eventueel worden herzien om er zeker van te zijn dat daarin de door de RFID-toepassing gebruikte soort informatie in aanmerking is genomen. Indien geen sprake is van zo'n PEB, moet rekening worden gehouden met de volgende componenten van het back-endsysteem:

- Toegangscontrolemechanismen met betrekking tot de soort persoonsgegevens en functionaliteit van de systemen.

- Controlemechanismen en beleidslijnen om ervoor te zorgen dat de exploitant persoonsgegevens in de RFID-toepassing koppelt op een wijze die consistent is met het PEB-verslag.

- Passende maatregelen ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens in de systemen en de communicatie-infrastructuur.

- Beleidslijnen over de bewaring en vernietiging van persoonsgegevens.

- Bestaan en uitvoering van controlemechanismen voor informatiebeveiliging, zoals:

    - Maatregelen met het oog op de veiligheid van netwerken en het transport van RFID-gegevens.

    - Maatregelen voor een betere beschikbaarheid van RFID-gegevens door middel van passende back-ups en herstel.

Bescherming van RFID-tags

Controlemechanismen voor **bescherming van RFID-tags** inzake de persoonlijke levenssfeer en persoonsgegevens moeten worden aangeduid. Zij zijn met name relevant voor RFID-toepassingen die gebruikmaken van RFID-tags met persoonsgegevens.

Deze controlemechanismen voor bescherming omvatten:

- Toegangscontrole tot functionaliteit en gegevens, waaronder authenticatie van lezers, schrijvers en onderliggende processen, en autorisatie om te handelen naar de RFID-tag.

- Methoden om de vertrouwelijkheid van de gegevens te waarborgen/aan de orde te stellen (bv. door versleuteling van de volledige RFID-tag of van keuzevelden).

- Methoden om de integriteit van de informatie te waarborgen/aan de orde te stellen.

- Bewaring van de gegevens na initiële verzameling (bv. bewaringstermijn, procedures voor gegevensverwijdering na afloop van de bewaringstermijn of voor gegevenswissing in de RFID-tag, procedures voor bewaring of schrapping van keuzevelden).

- De RFID-tag zelf tegen vervalsing bestand maken.

- Deactivering of verwijdering, indien vereist of anderszins bepaald.

Risicobeperking kan op gebruikers gebaseerde controlemechanismen omvatten die situaties aanpakken waarin andere behoeften of gevoeligheden inzake de persoonlijke levenssfeer aan de orde kunnen zijn. Deactivering of verwijdering zijn op dit moment de twee meest voorkomende vormen van risicobeperking voor eindgebruikers/klanten. Zij kunnen vereist zijn in het kader van een PEB-analyse, in bepaalde omstandigheden bij wet of als optie voor de klant na de verkoop ter bevordering van het vertrouwen. Daarnaast worden in de EG-aanbeveling over de bescherming van de persoonlijke levenssfeer en van persoonsgegevens inzake RFID-toepassingen bepaalde methodologieën en beste praktijken naar voren gebracht met betrekking tot deactivering of verwijdering in de winkel[4].

Verantwoordingsmaatregelen

Deze maatregelen zijn bedoeld om procedures voor gegevensbescherming wat betreft verantwoording te behandelen. Via deze maatregelen wordt de externe bewustmaking omtrent RFID-toepassingen vergroot.

- Zorgen voor een goede beschikbaarheid van een uitgebreid **informatiebeleid** waarin het onderstaande wordt vermeld:

    - Identiteit en adres van de exploitant van RFID-toepassingen.

    - Doel van de RFID-toepassing

    - Soorten gegevens die door de RFID-toepassing worden verwerkt, met name in het geval van verwerking van persoonsgegevens.

    - Of er al dan niet toezicht gehouden wordt op de locatie van de RFID-tags indien zij in handen zijn van een persoon.

    - Eventuele waarschijnlijke effecten op het gebied van persoonlijke levenssfeer en gegevensbescherming met betrekking tot het gebruik van RFID-tags in de RFID-toepassing en de beschikbare maatregelen om deze effecten te beperken.
- Zorgen voor beknopte, nauwkeurige en heldere **kennisgevingen** over de aanwezigheid van RFID-lezers, waarin het volgende is vermeld:

    - De identiteit van de exploitant van RFID-toepassingen.

[4] Punt 12/13 van de aanbeveling van de EC van 12 mei 2009. {SEC(2009) 585}: *een methode voor deactivering of verwijdering van tags dient onmiddellijk of in een later stadium kosteloos ter beschikking worden gesteld en betekent geenszins een vermindering of beëindiging van de juridische verplichtingen van de kleinhandelaar of producent ten opzichte van de consument.*

- Een aanspreekpunt voor personen om het informatiebeleid te verkrijgen.

- Vermelden of en hoe **verhaalmechanismen** ter beschikking worden gesteld:

  - Verantwoordelijke rechtsperso(o)n(en) van de exploitant van RFID-toepassingen (mogelijk één voor elk rechtsgebied of functioneringsgebied).

  - Contactgegevens van de persoon die of het kantoor dat belast is met de herziening van de beoordelingen en van de verdere toepasselijkheid van de technische en organisatorische maatregelen voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer.

  - Methoden voor informatieaanvraag (bv. methoden om de exploitant van RFID-toepassingen te bereiken voor vragen, verzoeken, klachten of uitoefening van rechten).

  - Methoden om bezwaar te maken tegen verwerking, om het recht van toegang tot persoonsgegevens uit te oefenen (inclusief het schrappen en corrigeren van persoonsgegevens), om toestemming in te trekken of controlemechanismen en andere keuzes te wijzigen met betrekking tot de verwerking van persoonsgegevens, indien vereist of anderszins bepaald.

  - Andere verhaalmethoden, indien vereist of anderszins bepaald.

Aanhangsel A: Verwijzingen

In dit aanhangsel staan verwijzingen naar formele documenten die zijn gebruikt bij de ontwikkeling van het kader.

- "Aanbeveling van de Commissie van 12 mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen", Commissie van de Europese Gemeenschappen, 12 mei 2009, C(2009) 3200, beschikbaar op: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:NL:PDF.

- "Begeleidend werkdocument van de diensten van de Commissie bij de aanbeveling van de Commissie over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen", samenvatting van de effectbeoordeling, Commissie van de Europese Gemeenschappen, 12 mei 2009, SEC(2009) 586, beschikbaar in het Engels op http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf.

- "Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens", Publicatieblad van de Europese Gemeenschappen, 23 november 1995, L 281, blz. 31, beschikbaar op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:NL:HTML.

- "Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)", Publicatieblad van de Europese Gemeenschappen, 31 juli 2002, L 201, blz. 37, beschikbaar op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:NL:PDF.

- "Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming", Publicatieblad van de Europese Unie, 18 december 2009, L 337, blz. 11, beschikbaar op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:NL:PDF.

- "Advies 4/2007 over het begrip persoonsgegevens", Groep gegevensbescherming artikel 29, 20 juni 2007, 01248/07/EN WP 136, beschikbaar op http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

- "Privacy Impact Assessment Handbook", beschikbaar op http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

- "Toestand inzake de uitvoering van Richtlijn 95/46 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens", beschikbaar op http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

- "Werkdocument over kwesties van gegevensbescherming in verband met RFID-technologie", Groep gegevensbescherming artikel 29, 19 januari 2005, 10107/05/EN WP 105, beschikbaar in het Engels op http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

Aanhangsel B: Verklarende woordenlijst

In het kader worden een aantal termen gebruikt met betrekking tot de begrippen "bescherming van de persoonlijke levenssfeer en persoonsgegevens" en tot de toepassing van RFID-technologie in verschillende contexten. Voor de toepassing van dit kader zijn de in Richtlijn 95/46/EG gegeven definities van toepassing inzake bescherming van de persoonlijke levenssfeer en persoonsgegevens.

De volgende definities hebben betrekking op de RFID-technologie en de toepassing ervan en zijn relevant voor het kader:

Persoon. Een natuurlijke persoon die in wisselwerking staat met of anderszins is betrokken bij een of meer componenten van een RFID-toepassing (bv. back-endsysteem, communicatie-infrastructuur, RFID-tag), maar die geen RFID-toepassing exploiteert of functies ervan gebruikt. In dit opzicht kan de persoon een andere zijn dan de gebruiker. Een persoon hoeft niet direct betrokken te zijn bij de werking van de RFID-toepassing, maar kan bijvoorbeeld louter een artikel bezitten dat een RFID-tag bevat.

Informatiebeveiliging. Het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

Toezicht. Het uitvoeren van een activiteit om de plaats, beweging, activiteiten of toestand van een persoon op te sporen, waar te nemen, te kopiëren of te registreren.

Persoonsgegevens. Iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon ("betrokkene"); als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

RFID-toepassing. Een toepassing die gegevens verwerkt door tags en lezers te gebruiken en ondersteund wordt door een back-endsysteem en een communicatie-netwerkinfrastructuur.

Exploitant van RFID-toepassingen. De natuurlijke of rechtspersoon, overheid, agentschap of elke ander instantie die alleen of gezamenlijk met anderen de doelstellingen en middelen bepaalt voor het exploiteren van een toepassing met inbegrip van de verantwoordelijken voor de verwerking van persoonsgegevens die gebruik maken van een RFID-toepassing.

Radiofrequentie-identificatie (RFID). Het gebruik van elektromagnetische golven of de koppeling van reactieve velden in de radiofrequentie van het spectrum voor de communicatie naar of van een RFID-tag met behulp van verschillende modulatie- of coderingstechnieken of alleen voor het aflezen van de identificatie van een RFID-tag of andere daarin opgeslagen gegevens.

RFID-lezer. Een vast of mobiel instrument voor gegevensvastlegging en -identificatie dat door middel van een elektromagnetische golf of de koppeling van reactieve velden in het radiospectrum van een of meerdere tags een respons in de vorm van gemoduleerde gegevens opwekt en teweegbrengt.

RFID-tag of "tag". Een RFID-apparaat dat een radiosignaal kan produceren of een RFID-apparaat dat een van een lees- of schrijfinstrument ontvangen dragersignaal terugkoppelt, terugstrooit of weerkaatst (afhankelijk van het soort apparaat) en moduleert.

RFID-taginformatie of informatie over de RFID-tag. De informatie in een RFID-tag die wordt verzonden wanneer de RFID-tag door een RFID-lezer wordt opgevraagd.

Gebruiker. In het bijzonder een gebruiker van RFID-toepassingen, d.w.z. een persoon (of andere entiteit, zoals een rechtspersoon) die in wisselwerking staat met een of meer componenten van een RFID-toepassing (bv. back-endsysteem, communicatie-infrastructuur, RFID-tag) met het oog op de exploitatie van een RFID-toepassing of het gebruik van een of meer functies ervan.