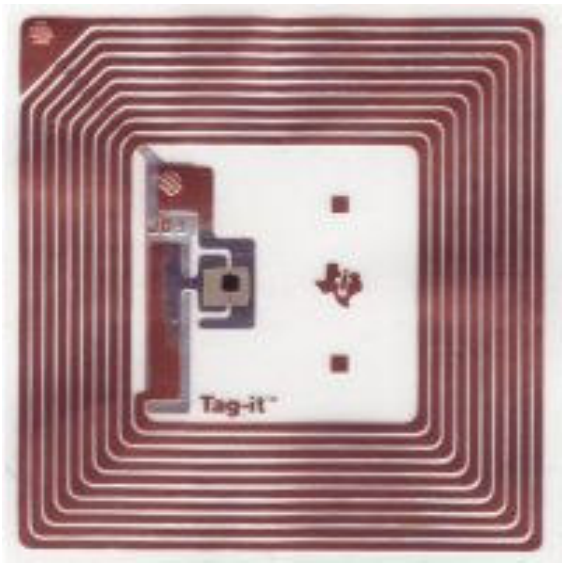
Resume af EU rammemodel for RFID PIA.



IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Resume af EU rammemodel for RFID PIA

Udgivet af:

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Publikationen kan hentes
på RFID i Danmarks
hjemmeside: http://www.rfididanmark.dk

Konsulent: Henrik Brandenborg Granau

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Resume af EU rammemodel for RFID PIA.

Indholdsfortegnelse

Resume af EU rammemodel for RFID PIA.

Baggrunden for den fælles rammemodel

Den 12. maj 2009 udgav EU Kommisionen en henstilling til medlemslandene vedrørende implementering af beskyttelsesprincipper for data og privatlivets fred i systemer, der anvender Radio Frekvens IDentifikation (RFID) teknologi.

Denne henstilling er beskrevet på dansk i dokumentet "EU Kommisionens RFID henstilling" (se www.rfididanmark.dk).

Henstillingen til medlemslandene har til formål at sikre, at vi i EU opnår alle de potentielle fordele, RFID teknologien indeholder, samtidig med at vi opretholder fuld respekt for privatlivet og beskyttelsen af personlige data.

I henstillingen anførte EU kommisionen, at der med repræsentation af alle relevante interessenter, skulle udarbejdes en fælles EU rammemodel for RFID Privatlivsimplikationsanalyser (PIA'er), samt at denne model skulle godkendes af Artikel 29 arbejdsgruppen vedrørende databeskyttelse.

Efter at en første model i 2010 var blevet afvist af Artikel 29 gruppen, blev en revideret rammemodel fremsendt til gruppen den 12. januar 2011.

Denne rammemodel, der er beskrevet i dette dokument, blev godkendt af arbejdsgruppen den 27. januar 2011.

Resume af EU rammemodel for RFID PIA.

Introduktion til koncepter, begreber og terminologi

Personhenførbare data kan lagres på RFID tags, men da en specifik RFID tag har et helt entydigt nummer, kan denne også benyttes til at knytte en RFID tag til personlige data lagret et andet sted i systemet.

Derfor skaber RFID teknologien mulighed for anvendelse til overvågning af personer via deres besiddelse af en eller flere genstande (eksempelvis tøj), der indeholder en RFID tag.

Fordi RFID teknologien kan være overalt og i praksis være usynlig, er der behov for en særlig opmærksomhed på beskyttelses-problemstillinger for data og privatlivets fred, når RFID teknologi tages i anvendelse.

Ved anvendelse af PIA'er for RFID systemer hjælpes den ansvarlige for RFID systemet med at sikre at love og regler vedr. datasikkerhed, herunder person-databeskyttelse, overholdes. Endvidere hjælper den med til at have styr på risici i forhold til brugere af RFID systemet - både mht. beskyttelse af data og privatlivets fred set ud fra en generel offentlig opfattelse, såvel som forbrugertillid specifikt.

PIA-processen er baseret på en risikostyrings-tilgang med fokus på de i EU henstillingen af 12. maj 2009 anførte risici vedr. beskyttelse af data og privatlivets fred, og under hensyntagen til gældende juridisk regelsæt og praksis.

Formålet med rammemodellen er at tjene som vejledning for RFID system ansvarlige til at kunne udføre PIA'er for specifikke RFID systemer, således som EU Kommisionen henstiller. Samtidig definerer rammemodellen form og indhold for de PIA Rapporter, hvor resultaterne fra PIA'en bliver dokumenteret.

Endvidere er det tanken, at rammemodellen kan anvendes til at udarbejde skabeloner (PIA Templates) for en system-type eller inden for en branche, således at ikke alle skal udvikle sin PIA fra bunden.

Rammemodellen beskriver processer for udførelse af en PIA for RFID systemer *forud* for idriftsættelse, samt specificerer omfanget af den tilhørende PIA Rapport.

Resume af EU rammemodel for RFID PIA.

PIA processen

Den ansvarlige for et RFID system skal udføre en PIA for hvert RFID system, der idriftsættes.

PIA processen har to faser:

1. **Indledende analyse:** ved at følge beskreven fremgangsmåde afgøres:
    a. Om en PIA for RFID systemet er påkrævet eller ej
    b. Om en komplet eller en reduceret PIA er nødvendig

2. **Risikovurdering:** hvor kriterier og emner i en komplet og en reduceret PIA gennemgås

Indledende analyse

I den indledende analyse følger man beslutningstræet, der er afbildet i Figur 1.

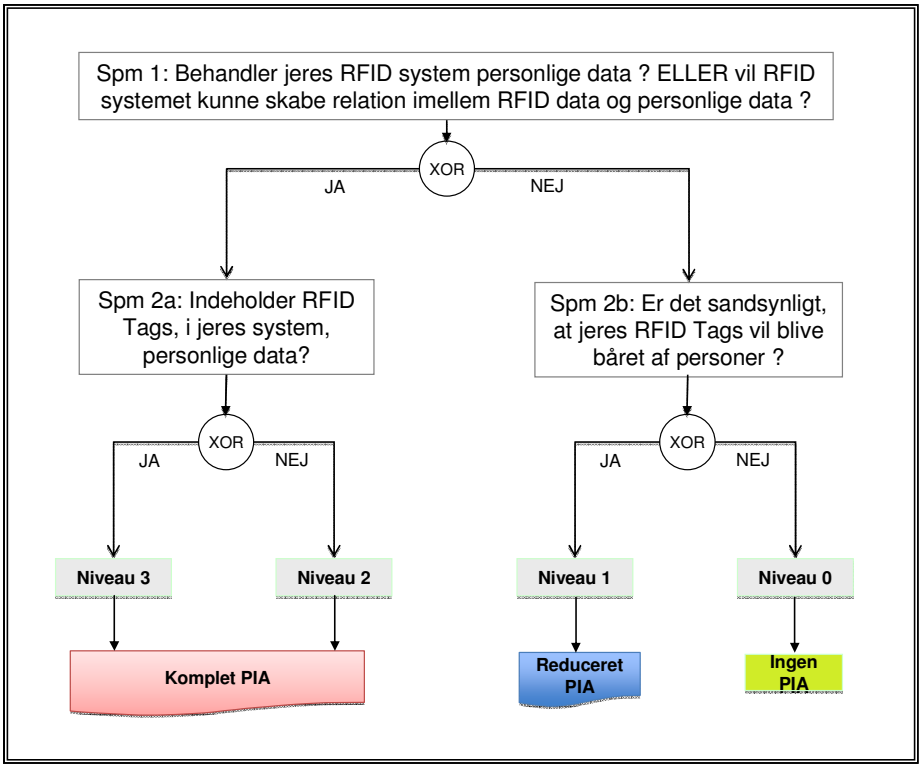
Dette vil hjælpe med at bestemme om en PIA er påkrævet, og i givet fald i hvilket omfang.

Niveauet (0-3) vil bestemme detaljeringsniveauet for den risikovurdering, der skal gennemføres (komplet eller reduceret PIA).

Den indledende analyse skal dokumenteres.

I den fælles EU rammemodel for RFID PIA af den 12. januar 2011 er der i **ANNEX I** en vejledning til hvilken information, der bør være i en PIA Rapport.

Resume af EU rammemodel for RFID PIA.



Figur 1: Beslutningstræ for om og på hvilket niveau man skal udføre en PIA

Selvom både niveau-2 og niveau-3 resulterer i en komplet PIA, vil de identificere forskellige risici og derfor også forskellige fremgangsmåder for sikkerheds-mæssige foranstaltninger.

Niveau-2 vil eksempelvis have et naturligt fokus på sikring af adgang til data lagret på servere, mens niveau-3 i tillæg til beskyttelse af data på servere også skal beskytte adgangen til data på RFID Tags.

Idet systemet behandler personlige data, er en høj detaljeringsgrad i risiko-vurderingen (komplet) nødvendig for at sikre, at de sikkerhedsmæssige foranstaltninger bliver gennemarbejdet.

I denne sammenhæng bør den RFID system ansvarlige også overveje hvorvidt det er sandsynligt, at informationen fra aflæsning af RFID Tags kan blive anvendt til andet end det oprindelige formål eller i andre sammenhænge.

En reduceret PIA følger den samme proces som en komplet, men med den lavere risiko profil er både omfang og detaljeringsniveau i såvel analyse som i rapporten mindre end ved den komplette PIA.

Risikovurdering

Formålet med risikovurderingen er at identificere potentielle risici for privatlivets fred, der kan forårsages af RFID systemet (ideelt set identificeres de potentielle risici tidligt i udviklingen af systemet), og at dokumentere, hvordan disse risici *proaktivt* er imødegået ved tekniske og organisatoriske kontroller.

På denne måde spiller en PIA en meget vigtig rolle ved overholdelsen af lovmæssige krav om persondata og privatlivets fred, og er samtidig et mål for at kunne vurdere, hvor effektive de indførte sikkerhedsmæssige foranstaltninger er.

For at spare både tid og penge anbefales det at gennemføre risikovurderingen i god tid forud for, at de endelige beslutninger vedrørende RFID systemets opbygning tages, således at tekniske sikkerhedsforanstaltninger kan blive bygget ind i systemet – allerede på design stadiet ('privacy by design').

I en risikovurderingsproces vægtes normalt sandsynligheden, for at hændelsen indtræffer med konsekvenserne, hvis den indtræffer. På denne måde fremkommer en naturlig prioritering af hvilke risici, der kræver mest opmærksomhed.

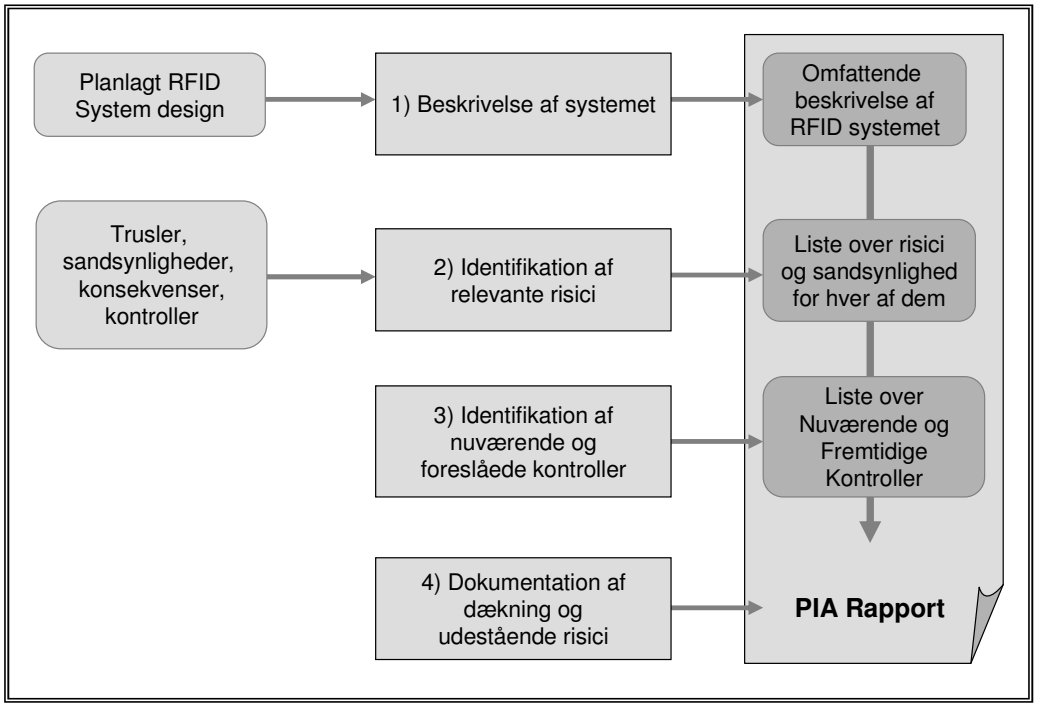
ANNEX II i den fælles EU rammemodel for RFID PIA af den 12. januar 2011 er de 'Privacy Targets', der er indbygget i EU's privacy direktiv, gengivet . Denne liste indeholder 9 beskrevne risici for privatlivets fred og vil være et udmærket udgangspunkt for en risikovurdering for det nye RFID system.

Risikoen for privatlivets fred kan enten være høj fordi RFID systemet kan være sårbart over for ondsindede angreb, eller fordi der ikke er etableret

organisatoriske procedurer. Risikoen kan også være lav, simpelthen fordi hændelsen er usandsynlig i systemet, eller fordi RFID systemet allerede er forhånds konfigureret til at inddrage hensynet til beskyttelse af privatlivets fred.

PIA processen har til formål at sikre, at alle potentielle risici overvejes mht. omfang, sandsynlighed og mulige imødegåelser. Resultatet af overvejelserne er en identifikation af de risici for privatlivets fred, det er nødvendigt at imødegå med effektive kontroller.

PIA processen er visualiseret i figur 2.



Figur 2: PIA processen

Resume af EU rammemodel for RFID PIA.

1) Beskrivelse af systemet.

Beskrivelsen af systemet bør give et omfattende og fyldestgørende billede af det samlede RFID system, dets omgivelser og systemsnitflader.

Systemets design, snitflader til andre systemer og informationsstrømme beskrives. Data flow diagrammer, der viser behandlingen af data, anbefales som visualisering.

Data strukturer skal også dokumenteres, således at potentiel sammenkædning af data kan blive analyseret.

I den fælles EU rammemodel for RFID PIA af den 12. januar 2011 er der i **ANNEX I** en vejledning til hvilke karakteristika, der foreslås medtaget ved beskrivelsen af et RFID system.

2) Identifikation af relevante risici.

Formålet med denne aktivitet er at identificere omstændigheder, der vil kunne true eller kompromittere personlige data. Dette gøres med fordel ved at benytte EU direktivet som vejledning i hvilke 'privacy targets', der skal adresseres. Risici kan være relateret til RFID systemets komponenter, til driftsmiljøet og til det datadelings- og behandlings miljø, som RFID systemet måtte være en del af.

I den fælles EU rammemodel for RFID PIA af den 12. januar 2011 er der i **ANNEX III** en liste over potentielle risici for privatlivets fred. Denne kan med fordel anvendes som vejledning til at sikre en systematisk identifikation af truslerne imod 'privacy targets' (EU rammemodel for RFID PIA af den 12. januar 2011 **ANNEX II**).

I tillæg til identifikation af risici kræver en PIA en relativ kvantificering af risiciene. Den ansvarlige for RFID systemet bør vurdere, hvor sandsynligt det er, at en hændelse indtræffer. Risiciene kan både opstå ved sandsynlig anvendelse af systemet, såvel som mulig misbrug af information – i særdeleshed, hvis RFID tags ikke er de-aktiveret, når de er overleveret til personer. Her henvises til EU Kommissionens RFID henstilling for yderligere problemstillinger i detailhandel.

Ved at sammenholde sandsynligheden, for at hændelsen indtræffer med konsekvenserne hvis den indtræffer, opnås, at man kan klassificere risiciene i tre kategorier: høj, middel og lav.

3) Identifikation af nuværende og foreslåede kontroller

Formålet med denne aktivitet er at analysere de kontroller, der allerede er etableret eller er planlagt etableret, for at minimere, omgå eller eliminere de identificerede risici for privatlivets fred.

Kontroller er enten af teknisk eller ikke-teknisk karakter. Tekniske kontroller er indbygget i RFID systemet gennem design og konfiguration – eks. parametre, mekanismer til kontrol af autencitet og krypteringsmetoder. Ikke-tekniske kontroller er på den anden side styrings- og driftsmæssige kontroller – eks. driftsprocedurer.

Kontroller kan karakteriseres som værende forebyggende eller opdagende. De første forhindrer angreb mod systemet, mens de andre kan sende advarsler ved angrebsforsøg.

De identificerede risici og de tilhørende risikoniveauer bør være bestemmende for, hvilke af de identificerede kontroller, der er relevante, og derfor skal etableres. PIA dokumentationen bør inkludere forklaring på, hvordan de enkelte kontroller er relateret til specifikke risici, samt en skriftlig vurdering af hvorvidt tiltagene gør, at en acceptabel risiko opnås.

I den fælles EU rammemodel for RFID PIA af den 12. januar 2011 er der i **ANNEX IV** medtaget en liste over eksempler på kontroller for RFID systemer.

4) Dokumentation af dækning og udestående risici

Når risikovurderingen er gennemført, skal resultaterne dokumenteres i en PIA Rapport sammen med øvrige bemærkninger vedrørende risici, kontroller og udestående risici.

Resume af EU rammemodel for RFID PIA.

Et RFID system er klar til idriftsættelse, når PIA processen er afsluttet uden væsentlige udestående risici. Når et RFID system ikke er klar til idriftsættelse på det givne stadie, skal der udarbejdes en specifik handlingsplan for ændringer, og en ny PIA vil skulle udføres, når systemet menes klar til idriftsættelse.

Interne procedurer og rapportering.

En ansvarlig for et RFID system bør have egne interne procedurer til at understøtte udførelsen af PIA'er :

- Udpege en person og/eller funktion i organisationen, der vil have ansvaret for at sikre udførelsen af diverse aktiviteter i PIA processen, samt dokumentationen af resultaterne
- Etablering af procedurer, der giver kriterier for vurdering og dokumentation af, om et RFID system er klar til idriftsættelse eller ej i forhold til rammemodellen og eventuelle relevante PIA skabeloner
- Planlægning af PIA processen, så der er afsat tilstrækkelig tid til at foretage ændringer i RFID systemet
- Internt review af PIA processen (inklusive den indledende analyse) og PIA Rapporten for check af konsistens med anden dokumentation af RFID systemet, så som system dokumentation, produkt dokumentation og eksempler på pakning af produkter og RFID tag implementering. Det interne review bør også sikre at konsekvenser og hændelser ved tidligere igangsatte RFID systemer bliver holdt op imod tidligere gennemførte PIA'er
- Gennemgang af alle relaterede fakta, som eksempelvis sikkerheds reviews og gennemgang af kontroller som dokumentation for, at RFID systemet har levet op til kravene
- Overvejelse og identifikation af faktorer, der vil kræve en ny eller revideret PIA Rapport. Dette bør omfatte større ændringer i systemet, udvidelse af funktionsområde, typer af information der behandles, informations-anvendelse, der svækker indbyggede kontroller, og indtrædelse af utilsigtede hændelser, der ikke var identificeret i den første PIA
- Konsultere interessenter. Meninger og feedback fra relevante interessenter for RFID systemet bør gives passende overvejelser ved review af PIA.

Resume af EU rammemodel for RFID PIA.

PIA'er er interne processer, der kan indeholde følsom information, der kan have sikkerhedsmæssige implikationer såvel som fortrolighedsmæssig information relateret til produkter og processer. Under hensyntagen til dette bør en PIA Rapport inkludere:

1. Beskrivelsen af RFID systemet (jf. ANNEX I i rammemodellen)
2. Dokumentation af de 4 aktivitetstrin i PIA processen

PIA Rapporten påføres navn og titel på personen, der underskriver som ansvarlig for indholdet.

PIA Rapporten bør herefter afleveres til den i organisationen udpegede ansvarlige person og/eller funktion jf. interne procedurer beskrevet ovenfor.

Resume af EU rammemodel for RFID PIA.

Ibrugtagning af PIA modellen.

EU Kommisionen vil sikre at udviklingen af retningslinier på EU niveau for informationssikkerhed i RFID systemer bliver baseret på eksisterende praksis og erfaringer fra medlemslandene, og opfordrer landene til at bidrage til denne proces samt at opmuntre private og offentlige organisationer til at deltage.

Såvel medlemslandene som alle interessenterne bør, især i den indledende fase for RFID udbredelse, yde en ekstra indsats for at sikre, at anvendelse af RFID monitoreres og individers rettigheder og frihed bliver respekteret.

Medlemslandene bør tage alle nødvendige tiltag til at bringe opmærksomhed på EU rammemodellen for RFID PIA hos alle interessenter, der er involveret i design og anvendelse af RFID systemer i samfundet.

EU rammemodellen for RFID PIA skal være taget i brug senest 6 måneder efter offentliggørelsen og godkendelsen fra Artikel 29 arbejdsgruppen. Det vil sige senest i juli 2011.

Resume af EU rammemodel for RFID PIA.

EU Kommisionens rammemodel for RFID PIA i sin fulde ordlyd kan hentes .....

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

Artikel 29 Data Protection Working Party har givet kommentarer i forbindelse med godkendelsen. De kan i deres fulde ordlyd hentes ....

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

EU Kommisionens RFID henstilling i sin fulde ordlyd kan hentes på EU's website:

http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf