

# Privatlivsimplicationsanalyse (PIA) for RFID.

---



**IT- og Telestyrelsen**  
Ministeriet for Videnskab  
Teknologi og Udvikling

# Privatlivsimplicationsanalyse (PIA) for RFID.

---

## Oplysning om privatlivsimplicationsanalyse (PIA) for RFID

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.rfid danmark.dk>

Konsulent: Henrik Brandenburg Granau



IT- og Telestyrelsen  
Ministeriet for Videnskab  
Teknologi og Udvikling

# Privatlivsimplicationsanalyse (PIA) for RFID.

---

## Indholdsfortegnelse

Hvorfor specifikt fokus på PIA for RFID teknologi ? .....	4
PIA proces og rapport .....	5
Mere information om RFID PIA .....	8



# Privatlivsimplicationsanalyse (PIA) for RFID.

---

## **HVORFOR SPECIFIKT FOKUS PÅ PIA FOR RFID TEKNOLOGI ?**

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 hjælper 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.



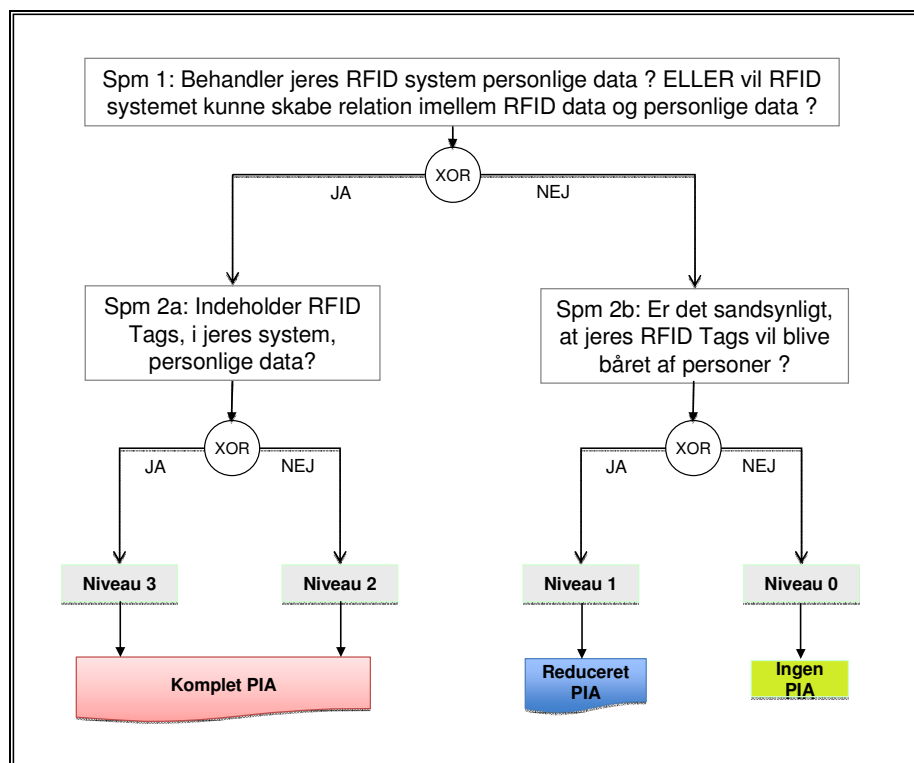
# Privatlivsimplicationsanalyse (PIA) for RFID.

## PIA PROCES OG RAPPORT

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

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

Dette vil hjælpe med at bestemme, om en PIA er påkrævet og i givet fald i hvilket omfang. Niveaue (0-3) vil bestemme detaljeringsniveauet for den risikovurdering, der skal gennemføres (komplet eller reduceret PIA).



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



# Privatlivsimplicationsanalyse (PIA) for RFID.

---

Den indledende analyse bør dokumenteres, og den bør på opfordring kunne stilles til rådighed for offentlige myndigheder vedr. datasikkerhed.

Selvom både niveau-2 og niveau-3 resulterer i en komplet PIA, vil de identificere forskellige risici og derfor også forskellige fremgangsmåder for sikkerhedsmæssige 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 risikovurderingen (komplet) nødvendig for at sikre, at de sikkerhedsmæssige foranstaltninger bliver gennemarbejdet.

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

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

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.

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').

PIA processen har til formål at sikre, at alle potentielle risici overvejes mht. omfang, sandsynlighed og mulige imødegåelser. Resultatet af overvejelserne er



# Privatlivsimplicationsanalyse (PIA) for RFID.

---

en identifikation af de risici for privatlivets fred, det er nødvendigt at imødegå med effektive kontroller.

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

Et RFID system er klar til idriftsættelse, når PIA processen er afsluttet uden væsentlige udestående risici.

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 har ansvaret for at sikre udførelsen af diverse aktiviteter i PIA processen, samt dokumentationen af resultaterne.

Det anbefales endvidere at konsultere interessenter. Meninger og feedback fra relevante interessenter for RFID systemet bør gives passende overvejelser ved review af PIA.



# Privatlivsimplicationsanalyse (PIA) for RFID.

---

## MERE INFORMATION OM RFID PIA

EU Kommissionen vil, 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.

EU Kommissionen har derfor fået udarbejdet en fælles rammemodel for RFID PIA.

Denne rammemodel er resumeret på dansk i dokumentet "Resume af EU rammemodel for RFID PIA" (se [www.rfididanmark.dk](http://www.rfididanmark.dk) ).

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

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180\\_annex\\_en.pdf](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](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf)

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

[http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf)

