

HENSTILLINGER

KOMMISSIONEN

KOMMISSIONENS HENSTILLING

af 12. maj 2009

om gennemførelse af principperne om beskyttelse af personoplysninger og privatlivets fred i forbindelse med anvendelse af radiofrekvensbaseret identifikation

(meddelt under nummer K(2009) 3200)

(2009/387/EF)

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 211,

som har hørt Den Europæiske Tilsynsførende for Databeskyttelse, og

som tager følgende i betragtning:

- (1) Radiofrekvensbaseret identifikation (RFID) er udtryk for en ny udvikling i informationsområdet, hvor genstande forsynet med mikroelektronik, der kan behandle data automatisk, i stigende grad bliver et fast led i hverdagen.
- (2) RFID bliver gradvist mere og mere udbredt og dermed en del af den enkeltes liv på en række områder som f.eks. logistik⁽¹⁾, sundhedsvæsen, offentlig transport, detailhandel (hvor RFID især medvirker til øget produktsikkerhed og hurtigere tilbagekaldelse af produkter), underholdning, arbejde, bompengeadministration, bagagehåndtering og rejsedokumenter.
- (3) RFID-teknologi kan blive en ny drivkraft for vækst og beskæftigelse og dermed yde et vigtigt bidrag til Lissabonstrategien: den rummer store økonomiske fordele i form af nye forretningsmuligheder, nedsatte omkostninger og øget effektivitet, særlig i kampen mod forfalskninger og i forvaltningen af elektronisk affald og farlige stoffer samt nyttiggørelse af produkter, når de er udtjente.
- (4) RFID-teknologien gør det muligt at behandle data, herunder personoplysninger, over korte afstande uden

fysisk kontakt eller synlig kommunikation mellem RFID-læseren/-skriveren og RFID-brikken, således, at denne kommunikation kan finde sted, uden at den berørte person er klar over det.

- (5) RFID-anvendelser giver mulighed for at behandle data vedrørende en identificeret eller identificerbar fysisk person, hvilket indebærer, at en fysisk person kan identificeres direkte eller indirekte. Disse anvendelser kan behandle personoplysninger, der er lagret i RFID-brikken, som f.eks. en persons navn, fødselsdato, adresse, biometriske data eller data, der forbinder et særligt RFID-artikelnnummer med personoplysninger et andet sted i systemet. Desuden kan teknologien bruges til at overvåge personer, der er i besiddelse af en eller flere genstande, som indeholder et RFID-artikelnnummer.
- (6) Da RFID-teknologien både er praktisk talt usynlig og kan anvendes overalt, er det nødvendigt at være særlig opmærksom på spørgsmålet om privatlivs- og databeskyttelse i forbindelse med brugen af RFID. Derfor bør der indbygges funktioner til beskyttelse af privatlivets fred og informationssikkerheden i RFID-anvendelser, før de vinder almen udbredelse (princippet om konstruktivt bestemt informationssikkerhed og privatlivsbeskyttelse).
- (7) De mange potentielle økonomiske og samfundsmæssige fordele ved RFID vil kun blive realiseret, hvis der træffes effektive foranstaltninger for at beskytte personoplysninger og privatlivets fred og de dermed forbundne etiske principper, der står i centrum for debatten om offentlig accept af RFID.
- (8) Medlemsstaterne og de berørte parter bør — især i denne indledende fase af indførelsen af RFID — bestræbe sig yderligere på at sikre, at RFID-anvendelser overvåges, og at individets rettigheder og friheder respekteres.

(¹) KOM(2007) 607 endelig.

- (9) I en meddelelse af 15. marts 2007, »Radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme«⁽¹⁾, bekendtgjorde Kommissionen, at den ville udstede en eller flere henstillinger om beskyttelse af personoplysninger og privatlivets fred i RFID-anvendelser for at skabe klarhed og opstille retningslinjer på dette område.
- (10) De rettigheder og forpligtelser vedrørende beskyttelse af personoplysninger og fri udveksling af sådanne oplysninger, der er fastsat i Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger⁽²⁾ og i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation)⁽³⁾, gælder også fuldt ud for brugen af RFID-anvendelser, der behandler personoplysninger.
- (11) De principper, der er fastlagt i Europa-Parlamentets og Rådets direktiv 1999/5/EF af 9. marts 1999 om radio- og teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse⁽⁴⁾, bør finde anvendelse i forbindelse med udvikling af RFID-anvendelser.
- (12) Udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse⁽⁵⁾ opstiller retningslinjer for, hvordan produkter, der er forsynet med RFID-brikker, og som leveres til privatpersoner, skal behandles; desuden efterlyser den konsekvensvurderinger vedrørende privatlivs- og databeskyttelsesaspekterne med henblik på at udpege og udvikle de »bedste tilgængelige teknikker« til at beskytte privatlivets fred og informationssikkerheden i RFID-systemer.
- (13) Operatører af RFID-anvendelser bør tage alle rimelige skridt til at sikre, at data ikke kan knyttes til en identificeret eller identificerbar fysisk person ved hjælp af et middel, der med sandsynlighed vil blive brugt enten af operatøren eller en anden person, medmindre disse data behandles i overensstemmelse med gældende principper og retlige bestemmelser om databeskyttelse.
- (14) Kommissionens meddelelse af 2. maj 2007 om bedre databeskyttelse med teknologier til beskyttelse af privatlivet⁽⁶⁾ opstiller klare tiltag for at nå målsætningen om at reducere behandlingen af personoplysninger til det mindst mulige og slette eller ændre navneangivelser, inden sådanne data bruges, hvor dette er muligt, ved at støtte udviklingen af teknologier til beskyttelse af privatlivets fred samt udbredelsen heraf blandt registeransvarlige og privatpersoner.
- (15) Kommissionens meddelelse af 31. maj 2006, »En strategi for et sikkert informationssamfund — Dialog, partnerskab og myndiggørelse«⁽⁷⁾ anerkender, at mangfoldighed, åbenhed, interoperabilitet, brugervenlighed og konkurrence er nøgledrivkræfter for et sikkert informationssamfund; endvidere fremhæves medlemsstaternes og de offentlige administrationers rolle i indsatsen for at skabe øget bevidsthed om sikkerhedsaspekterne og fremme god sikkerhedspraksis, og parterne i den private sektor opfordres til at tage initiativ til at arbejde hen imod prismæssigt overkommelige sikkerhedscertificeringsordninger, der omfatter produkter, processer og tjenester, og som opfylder EU-specifikke behov, navnlig hvad angår beskyttelse af privatlivets fred.
- (16) Rådets resolution af 22. marts 2007⁽⁸⁾ om en strategi for et sikkert informationssamfund i Europa opfordrer medlemsstaterne til at udvise den fornødne opmærksomhed over for behovet for at forebygge og bekæmpe nye og eksisterende sikkerhedstrusler mod elektroniske kommunikationsnet.
- (17) Der bør opstilles en ramme på fællesskabsplan for gennemførelse af konsekvensvurderinger vedrørende privatlivs- og databeskyttelse for at sikre, at bestemmelserne i denne henstilling følges ensartet i alle medlemsstater. Udformningen af en sådan ramme bør tage udgangspunkt i eksisterende praksis og erfaringer fra medlemsstaterne, tredjelande og det arbejde, der udføres af Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)⁽⁹⁾.
- (18) Kommissionen vil sørge for, at der udarbejdes retningslinjer på fællesskabsplan for forvaltning af informationssikkerheden i forbindelse med RFID-anvendelser på grundlag af eksisterende praksis og erfaringer fra medlemsstaterne og tredjelande. Medlemsstaterne bør bidrage til denne proces og tilskynde private organisationer og offentlige myndigheder til at deltage i den.
- (19) En vurdering af konsekvenserne for beskyttelsen af personoplysninger og privatlivets fred, der gennemføres af operatøren, inden en RFID-anvendelse sættes i værk, vil tilvejebringe de oplysninger, der er nødvendige for at iværksætte passende beskyttelsesforanstaltninger. Sådanne foranstaltninger bør overvåges og tages op til fornyet overvejelse gennem hele RFID-anvendelsens levetid.
- (20) I detailhandelsektoren bør en vurdering af konsekvenserne for beskyttelsen af personoplysninger eller privatlivets fred af produkter, der indeholder RFID-brikker, som sælges til forbrugere, omfatte de oplysninger, der er nødvendige for at afgøre, om der er sandsynlighed for, at beskyttelsen af personoplysninger eller privatlivets fred bringes i fare.

(1) KOM(2007) 96 endelig.

(2) EFT L 281 af 23.11.1995, s. 31.

(3) EFT L 201 af 31.7.2002, s. 37.

(4) EFT L 91 af 7.4.1999, s. 10.

(5) EUT C 101 af 23.4.2008, s. 1.

(6) KOM(2007) 228 endelig.

(7) KOM(2006) 251 endelig.

(8) EUT C 68 af 24.3.2007, s. 1.

(9) Artikel 2, stk. 1, i Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 (EUT L 77 af 13.3.2004, s. 1).

- (21) Brugen af internationale standarder som dem, der udarbejdes af Den Internationale Standardiseringsorganisation (ISO), adfærdskodekser og bedste praksis, der er i overensstemmelse med EU's lovrammer, kan gøre det lettere at styre foranstaltningerne til beskyttelse af informationsikkerheden og privatlivets fred gennem hele den RFID-støttede forretningsproces.
- (22) RFID-anvendelser, der har konsekvenser for befolkningen i almindelighed, f.eks. elektroniske billetter til offentlig transport, kræver passende beskyttelsesforanstaltninger. RFID-anvendelser, der berører enkeltpersoner, f.eks. biometriske identifikationsdata og sundhedsoplysninger, er særlig kritiske, når det gælder informationssikkerhed og privatlivsbeskyttelse, og kræver derfor særlig opmærksomhed.
- (23) Samfundet som helhed må være klar over, hvilke forpligtelser og rettigheder der gælder i forbindelse med brugen af RFID-anvendelser. De parter, der tager teknologien i brug, bærer derfor et ansvar for at informere den enkelte om brugen af disse anvendelser.
- (24) Øget bevidsthed i offentligheden og blandt små og mellemstore virksomheder om egenskaberne ved og mulighederne i RFID vil gøre det muligt at høste det økonomiske udbytte af denne teknologi, samtidig med at risikoen for, at den udnyttes til skade for offentligheden, mindskes, og teknologien derved vinder større accept.
- (25) Kommissionen vil bidrage både direkte og indirekte til gennemførelsen af denne henstilling ved at fremme dialog og samarbejde mellem parterne, særlig via rammeprogrammet for konkurrenceevne og innovation, jf. Europa-Parlamentets og Rådets afgørelse nr. 1639/2006/EF ⁽¹⁾, og via det syvende forskningsramme-program, jf. Europa-Parlamentets og Rådets afgørelse nr. 1982/2006/EF ⁽²⁾.
- (26) Det er afgørende, at der på fællesskabsplan forskes i og udvikles billig teknologi til beskyttelse af privatlivets fred og informationssikkerheden, for at denne teknologi kan vinde større udbredelse under acceptable betingelser.
- (27) I denne henstilling overholdes de grundlæggende rettigheder og de principper, som bl.a. Den Europæiske Unions charter om grundlæggende rettigheder anerkender. Henstillingen tilsigter især, at retten til privat- og familielivets fred samt beskyttelsen af personoplysninger respekteres fuldt ud,

HENSTILLER:

Anvendelsesområde

- Denne henstilling opstiller retningslinjer for medlemsstaterne for, hvordan RFID-anvendelser udformes og anvendes på en lovlig samt etisk og socialt acceptabel måde, med respekt for retten til privatlivets fred og garanti for, at personoplysninger beskyttes.
- Henstillingen indeholder retningslinjer for, hvilke foranstaltninger der skal træffes med henblik på indførelse af RFID-anvendelser for at sikre, at national lovgivning til gennemførelse af direktiv 95/46/EF, 1999/5/EF og 2002/58/EF overholdes, hvor det er relevant, når sådanne anvendelser tages i brug.

Definitioner

- I denne henstilling gælder definitionerne i direktiv 95/46/EF. Endvidere forstås ved:
 - »radiofrekvensbaseret identifikation« (RFID): brug af elektromagnetiske bølger eller induktiv kobling i radiofrekvensdelen af det elektromagnetiske spektrum til at kommunikere til eller fra en RFID-brik ved hjælp af forskellige modulations- og kodningssystemer, således at RFID-brikkens identitet eller andre data, der er lagret i den, kan læses entydigt
 - »RFID-brik«: RFID-udstyr, der enten er i stand til at frembringe et radiosignal, eller som genkobler, tilbagespreder eller reflekterer (alt afhængigt af udstyrets art) og dermed modulerer et bærersignal fra en RFID-læser/-skriver
 - »RFID-læser/-skriver«: fast eller mobilt udstyr til datafangst og -identifikation, der anvender radiobølger eller induktiv kobling til at stimulere og frembringe et moduleret datasvar fra en RFID-brik eller gruppe af brikker
 - »RFID-anvendelse« eller »anvendelse«: en anvendelse, der behandler data ved hjælp af RFID-brikker og RFID-læsere/-skrivere, og som bygger på et back-end-system og en netbaseret kommunikationsinfrastruktur
 - »operatør af RFID-anvendelser« eller »operatør«: den fysiske eller juridiske person, offentlige myndighed, institution eller andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke midler en RFID-anvendelse må drives, herunder forvaltere af personoplysninger, der benytter en RFID-anvendelse

⁽¹⁾ EUT L 310 af 9.11.2006, s. 15.

⁽²⁾ EUT L 412 af 30.12.2006, s. 1.

- f) »informationssikkerhed«: bevarelse af oplysningers fortrolighed, integritet og disponibilitet
- g) »overvågning«: enhver aktivitet, der udføres for at afsløre, observere, kopiere eller registrere en persons placering, bevægelser, aktiviteter eller tilstand.

Konsekvensvurderinger vedrørende privatlivs- og databeskyttelse

4. Medlemsstaterne bør sikre, at erhvervslivet i samarbejde med relevante parter fra civilsamfundet opstiller en ramme for konsekvensvurderinger vedrørende privatlivs- og databeskyttelse. Denne ramme bør forelægges for Artikel 29-gruppen vedrørende Beskyttelse af Personoplysninger til godkendelse senest 12 måneder efter denne henstillings offentliggørelse i *Den Europæiske Unions Tidende*.
5. Medlemsstaterne bør sikre, at operatører uanset deres forpligtelser i henhold til direktiv 95/46/EF:
- foretager en vurdering af, hvilke konsekvenser indførelsen af RFID-anvendelsen vil få for beskyttelsen af personoplysninger og privatlivets fred, herunder af, om anvendelsen kan bruges til at overvåge enkeltpersoner. Vurderingens detaljeringsgrad bør stå i et rimeligt forhold til de trusler mod privatlivets fred, der kan være forbundet med anvendelsen
 - træffe passende tekniske og organisatoriske foranstaltninger for at sikre, at personoplysninger og privatlivets fred beskyttes
 - udpege en person eller gruppe af personer, der får ansvaret for at gennemgå vurderingerne og afgøre, om de tekniske og organisatoriske foranstaltninger fortsat er egnede til at sikre, at personoplysninger og privatlivets fred beskyttes
 - stille vurderingen til rådighed for den kompetente myndighed, mindst seks uger før anvendelsen indføres
 - gennemføre ovenstående bestemmelser i overensstemmelse med rammen for konsekvensvurderinger vedrørende privatlivs- og databeskyttelse, jf. punkt 4, så snart denne ligger fast.

Informationssikkerhed

6. Medlemsstaterne bør bistå Kommissionen med at finde frem til, hvilke RFID-anvendelser der kan medføre trusler mod informationssikkerheden, som har konsekvenser for

offentligheden. For sådanne anvendelser bør medlemsstaterne sikre, at operatørerne sammen med de kompetente nationale myndigheder og civilsamfundsorganisationer opstiller nye ordninger eller anvender eksisterende ordninger, som f.eks. certificering eller selvevaluering blandt operatørerne, til at påvise, at der tilvejebringes et tilfredsstillende niveau af informationssikkerhed og beskyttelse af privatlivets fred set i forhold til de risici, der vurderes at være.

Oplysninger og åbenhed omkring brug af RFID

7. Uden at det tilsidesætter registeransvarliges forpligtelser i henhold til direktiv 95/46/EF og 2002/58/EF, bør medlemsstaterne sikre, at operatører udarbejder og offentliggør et sæt kortfattede, nøjagtige og letforståelige oplysninger for hver af deres anvendelser. Disse oplysninger bør som minimum omfatte:
- operatørens navn og adresse
 - formålet med anvendelsen
 - hvilke data der behandles af anvendelsen, særlig hvorvidt der er tale om personoplysninger, og hvorvidt RFID-brikkernes placering vil blive overvåget
 - et resumé af konsekvensvurderingen vedrørende privatlivs- og databeskyttelse
 - de sandsynlige trusler mod privatlivets fred, hvis sådanne eksisterer, i forbindelse med brugen af RFID-brikker i anvendelsen, og hvilke skridt den enkelte kan tage for at modvirke disse trusler.
8. Medlemsstaterne bør sikre, at operatører af RFID-anvendelser tager skridt til at informere den enkelte om tilstedeværelsen af RFID-læsere/-skrivere ved hjælp af et fælles europæisk kendemærke, der udformes af de europæiske standardiseringsorganisationer med bistand fra de berørte parter. Kendemærket bør omfatte operatørens navn og en kontaktadresse, hvor man kan få udleveret ovennævnte oplysninger om anvendelsen.

RFID-anvendelser i detailhandelen

9. Operatører af RFID-anvendelser bør informere den enkelte om tilstedeværelsen af RFID-brikker, der er anbragt på eller indbygget i produkter, ved hjælp af et fælles europæisk kendemærke, der udformes af de europæiske standardiseringsorganisationer med bistand fra de berørte parter.

10. Når operatøren af en anvendelse gennemfører konsekvensvurderingen vedrørende privatlivs- og databeskyttelse, jf. punkt 4 og 5, bør vedkommende specifikt undersøge, om RFID-brikker, der er anbragt på eller indbygget i produkter, som sælges til forbrugerne via detailhandlere, der ikke er operatører af den pågældende anvendelse, udgør en trussel mod privatlivets fred eller beskyttelsen af personoplysninger.
11. Detailhandlere bør deaktivere eller fjerne de RFID-brikker, der benyttes i deres RFID-anvendelser, ved salgsstedet, medmindre forbrugerne efter at være blevet gjort opmærksomme på oplysningerne om anvendelsen, jf. punkt 7, giver deres samtykke til, at RFID-brikkerne forbliver aktive. Ved deaktivering forstås enhver proces, der afbryder forbindelserne mellem en RFID-brik og dens omgivelser, og som ikke kræver nogen aktiv indsats fra forbrugers side. Deaktivering eller fjernelse af RFID-brikker bør foretages af detailhandleren øjeblikkeligt og uden omkostninger for forbrugeren. Forbrugerne bør kunne kontrollere, at en RFID-brik rent faktisk er blevet deaktiveret eller fjernet.
12. Punkt 11 bør ikke finde anvendelse, hvis konsekvensvurderingen vedrørende privatlivs- og databeskyttelse konkluderer, at RFID-brikker, der anvendes i et detailhandelsprodukt, og som ikke deaktiveres eller fjernes ved salgsstedet, ikke udgør en sandsynlig trussel mod privatlivets fred eller beskyttelsen af personoplysninger. Detailhandlerne bør dog tilbyde gratis og lettilgængelige midler til øjeblikkeligt eller på et senere tidspunkt at deaktivere eller fjerne sådanne RFID-brikker.
13. Deaktivering eller fjernelse af RFID-brikker bør ikke indebære, at detailhandlerens eller producentens retlige forpligtelser over for forbrugeren indskrænkes eller ophører.
14. Punkt 11 og 12 bør kun gælde for detailhandlere, der er operatører af RFID-anvendelser.

Oplysningsforanstaltninger

15. Medlemsstaterne bør i samarbejde med industrien, Kommissionen og andre berørte parter tage passende skridt til at oplyse og bevidstgøre offentlige myndigheder og virksomheder, især små og mellemstore virksomheder, om de potentielle fordele og risici, der er forbundet med brugen af RFID-teknologi. Der bør især lægges vægt på spørgsmålene om informationssikkerhed og privatlivets fred.

16. Medlemsstaterne bør i samarbejde med industrien, civilsamfundets organisationer, Kommissionen og andre berørte parter finde og fremlægge eksempler på god praksis for iværksættelse af RFID-anvendelser med det formål at oplyse og bevidstgøre befolkningen som helhed. De bør også træffe passende foranstaltninger, f.eks. i form af storstilede pilotprojekter, for at øge kendskabet til RFID-teknologien og de fordele, risici og mulige konsekvenser, der er forbundet med brugen heraf, som en forudsætning for en videre udbredelse af denne teknologi.

Forskning og udvikling

17. Medlemsstaterne bør samarbejde med industrien, relevante parter fra civilsamfundet og Kommissionen om at stimulere og støtte indførelsen af princippet om konstruktivt bestemt informationssikkerhed og privatlivsbeskyttelse på et tidligt trin i udviklingen af RFID-anvendelser.

Opfølgning

18. Medlemsstaterne bør træffe alle nødvendige foranstaltninger for at gøre alle parter, der er involveret i udformning og drift af RFID-anvendelser i Fællesskabet, opmærksomme på denne henstilling.
19. Medlemsstaterne bør underrette Kommissionen om, hvilke foranstaltninger de træffer for at efterkomme denne henstilling, senest 24 måneder efter henstillingens offentliggørelse i *Den Europæiske Unions Tidende*.
20. Senest tre år efter henstillingens offentliggørelse i *Den Europæiske Unions Tidende* forelægger Kommissionen en rapport om gennemførelsen af henstillingen, dens virkning og betydning for operatører og forbrugere, særlig for så vidt angår de foranstaltninger, der anbefales i punkt 9-14.

Adressater

21. Denne henstilling er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 12. maj 2009.

På Kommissionens vegne
Viviane REDING
Medlem af Kommissionen