REKOMMENDATIONER

KOMMISSIONEN

KOMMISSIONENS REKOMMENDATION

av den 12 maj 2009

om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID)

[delgivet med nr K(2009) 3200]

(2009/387/EG)

EUROPEISKA GEMENSKAPERNAS KOMMISSION UTFÄRDAR DENNA REKOMMENDATION

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 211,

efter samråd med Europeiska datatillsynsmannen, och

av följande skäl:

(1) Radiofrekvensidentifiering (RFID) markerar en ny utveckling i informationssamhället, där föremål som är utrustade med mikroelektronik som medger automatisk databehandling blir allt vanligare i vardagen.

(2) Användningen av radiofrekvensidentifiering ökar och blir därmed en del av individens liv inom en rad olika områden, exempelvis logistik [1], hälsovård, kollektivtrafik, detaljhandel (framför allt när det gäller att förbättra produktsäkerheten och återkalla produkter snabbare), underhållningsbranschen, i arbetet, vägavgiftssystem, bagagehantering och resehandlingar.

(3) RFID-tekniken har potential att bli en ny drivkraft för tillväxt och arbetstillfällen och kan således bidra på ett mycket positivt sätt till Lissabonstrategin på grund av de mycket lovande utsikterna i ekonomiskt hänseende. RFID-tekniken kan således bidra till att skapa nya affärsmöjligheter och kan medföra kostnadsminskningar och ökad effektivitet, särskilt när det gäller att bekämpa förfalskning, hantera ”e-avfall” och farliga material och vid återvinningen av produkter i slutet på deras livscykel.

(4) RFID-tekniken möjliggör behandling av uppgifter, inklusive personuppgifter, över korta distanser utan fysisk kontakt eller synlig interaktion mellan läsaren eller skrivaren och taggen, vilket innebär att denna interaktion kan ske utan att individen är medveten om det.

(5) RFID-tillämpningar kan behandla data om en identifierad eller identifierbar fysisk person, vilket innebär att en fysisk person kan identifieras direkt eller indirekt. De kan behandla personuppgifter som lagrats på taggen såsom en persons namn, födelsedatum eller adress eller biometriska uppgifter eller uppgifter som kopplar ett visst RFID-nummer till personuppgifter som är lagrade på en annan plats i systemet. Dessutom kan RFID-tekniken användas för övervakning av enskilda personer genom att de bär ett eller flera föremål som innehåller ett RFID-nummer.

(6) På grund av att RFID-tillämpningar kan finnas överallt, samtidigt som de är praktiskt taget osynliga, är det viktigt att uppmärksamma integritets- och dataskyddsfrågorna vid införandet av RFID. Följaktligen bör funktioner för integritetsskydd och informationssäkerhet byggas in i RFID-tillämpningar innan de börjar användas allmänt (principen ”security and privacy-by-design”).

(7) Det kommer endast att vara möjligt att utnyttja de många ekonomiska och sociala fördelarna med radiofrekvensidentifiering om effektiva åtgärder vidtas för att skydda personuppgifter, integriteten och de etiska principer som är förknippade med RFID och som står i centrum för debatten om allmänhetens acceptans av RFID.

(8) Medlemsstaterna och de berörda intressenterna bör, särskilt i den inledande fasen av genomförandet av RFID-tekniken, göra ytterligare insatser för att se till att RFID-tillämpningar övervakas och att individens rättigheter och friheter respekteras.

[1] KOM(2007) 607 slutlig.

(9) I sitt meddelande av den 15 mars 2007 – ”Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi” ([1]) – förklarade kommissionen att den skulle ge klargöranden och utfärda riktlinjer om skyddet av personuppgifter och privatlivet i samband med RFID-tillämpningar genom en eller flera rekommendationer.

(10) Rättigheterna och skyldigheterna när det gäller skyddet av personuppgifter och det fria flödet av sådana uppgifter gäller fullt ut för RFID-tillämpningar som behandlar personuppgifter enligt Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([2]) och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) ([3]).

(11) De principer som fastställs i Europaparlamentets och rådets direktiv 1999/5/EG av den 9 mars 1999 om radioutrustning och teleterminalutrustning och om ömsesidigt erkännande av utrustningens överensstämmelse ([4]) bör även tillämpas i utvecklingen av RFID-tillämpningar.

(12) I yttrandet från Europeiska datatillsynsmannen ([5]) ges vägledning om hur produkter ska hanteras som innehåller taggar som innehas av enskilda personer. Datatillsynsmannen efterlyser konsekvensanalyser avseende integritets- och säkerhetsaspekterna för att identifiera och utveckla ”bästa tillgängliga teknik” i syfte att skydda integriteten och säkerheten i RFID-system.

(13) Operatörer av RFID-tillämpningar bör vidta alla rimliga åtgärder för att se till att uppgifterna i fråga inte kan knytas till en identifierad eller identifierbar fysisk person genom något medel som sannolikt kan användas av antingen RFID-operatören eller någon annan person, om inte sådana uppgifter behandlas i enlighet med de tillämpliga principerna och rättsliga bestämmelserna om dataskydd.

(14) I sitt meddelande av den 2 maj 2007 om främjande av dataskydd genom integritetsfrämjande teknik ([6]) fastställer kommissionen tydliga åtgärder för att nå målet att minimera behandlingen av personuppgifter och där så är möjligt använda avidentifierade eller pseudonymförsedda uppgifter genom att stödja utvecklingen av integritetsfrämjande teknik och dess användning av registeransvariga och enskilda personer.

(15) I sitt meddelande av den 31 maj 2006 – ”En strategi för ett säkert informationssamhälle – ’Dialog, partnerskap och användarinflytande’” ([7]) – lyfter kommissionen fram mångfald, öppenhet, driftskompatibilitet, användarvänlighet och konkurrens som viktiga drivfjädrar för ett säkert informationssamhälle och betonar medlemsstaternas och de offentliga förvaltningarnas roll för att förbättra kunskapen och främja god praxis på säkerhetsområdet. Kommissionen uppmanar även intressenter från den privata sektorn att sträva efter system för säkerhetscertifiering för produkter, processer och tjänster till rimliga kostnader som kan tillgodose EU:s särskilda behov, inte minst när det gäller respekten för privatlivet.

(16) I rådets resolution av den 22 mars 2007 om en strategi för ett säkert informationssamhälle i Europa ([8]), uppmanas medlemsstaterna att rikta vederbörlig uppmärksamhet på behovet av att förebygga och bekämpa nya och befintliga säkerhetshot mot elektroniska kommunikationsnät.

(17) För att se till att denna rekommendation följs på ett enhetligt sätt i alla medlemsstater är det nödvändigt att utforma en ram på gemenskapsnivå för konsekvensanalyser avseende integritets- och dataskydd. Arbetet med att ta fram en sådan ram bör bygga på befintlig praxis och den erfarenhet som har vunnits i medlemsstaterna och i tredjeländer samt på det arbete som genomförs av Europeiska byrån för nät- och informationssäkerhet (Enisa) ([9]).

(18) Kommissionen kommer att se till att riktlinjer tas fram på gemenskapsnivå om hanteringen av informationssäkerhetsaspekter för RFID-tillämpningar. Riktlinjerna kommer att bygga på befintlig praxis och erfarenheter som vunnits i medlemsstaterna och tredjeländer. Medlemsstaterna bör bidra till denna process och även uppmana privata enheter och myndigheter att delta.

(19) En utvärdering om konsekvenserna avseende integritets- och dataskyddet, genomförd av operatören innan en RFID-tillämpning tas i drift, kommer att ge den information som krävs för att man ska kunna vidta lämpliga skyddsåtgärder. Sådana åtgärder bör övervakas och ses över under RFID-tillämpningens livstid.

(20) Inom detaljhandeln bör en utvärdering om konsekvenserna avseende integritets- och dataskyddet, för produkter som innehåller taggar och som säljs till konsumenter, ge den information som är nödvändig för att man ska kunna avgöra om det föreligger sannolika hot mot integriteten eller skyddet av personuppgifter.

([1]) KOM(2007) 96 slutlig.
([2]) EGT L 281, 23.11.1995, s. 31.
([3]) EGT L 201, 31.7.2002, s. 37.
([4]) EGT L 91, 7.4.1999, s. 10.
([5]) EUT C 101, 23.4.2008, s. 1.
([6]) KOM(2007) 228 slutlig.
([7]) KOM(2006) 251 slutlig.
([8]) EUT C 68, 24.3.2007, s. 1.
([9]) Artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 460/2004 (EUT L 77, 13.3.2004, s. 1).

(21) Användning av internationella standarder, t.ex. de som har tagits fram av Internationella standardiseringsorganisationen (ISO), samt av uppförandekoder och bästa praxis som är förenlig med EU:s regelverk, kan bidra till förvaltningen av åtgärder för informationssäkerhet och integritetsskydd inom hela den RFID-stödda affärsprocessen.

(22) RFID-tillämpningar som har konsekvenser för allmänheten, såsom elektroniska biljetter inom kollektivtrafiken, kräver lämpliga skyddsåtgärder. RFID-tillämpningar som påverkar enskilda personer genom att de till exempel behandlar biometriska identifieringsuppgifter eller hälsouppgifter, är särskilt känsliga när det gäller informationssäkerheten och integritetsskyddet, och kräver därför särskild uppmärksamhet.

(23) Hela samhället måste känna till de skyldigheter och rättigheter som gäller för användningen av RFID-tillämpningar. De parter som inför tekniken har därför ett ansvar att tillhandahålla enskilda personer information om användningen av dessa tillämpningar till.

(24) Genom att öka allmänhetens och små och medelstora företags kunskap om RFID-teknikens funktioner och möjliga användningsområden, blir det möjligt att utnyttja teknikens ekonomiska potential, samtidigt som man minskar riskerna för att tekniken används till nackdel för allmänintresset, vilket i sin tur ökar acceptansen för RFID.

(25) Kommissionen kommer direkt och indirekt att bidra till genomförandet av denna rekommendation genom att främja dialog och samarbete mellan de berörda intressenterna, särskilt genom ramprogrammet för konkurrenskraft och innovation (CIP) som inrättades genom Europaparlamentets och rådets beslut nr 1639/2006/EG ([1]) och sjunde ramforskningsprogrammet (FP7) som inrättades genom Europaparlamentets och rådets beslut nr 1982/2006/EG ([2]).

(26) Forskning och utveckling om billig integritetsfrämjande teknik och informationssäkerhetsteknik är av central betydelse på gemenskapsnivå för att främja ett mer omfattande införande av dessa tekniker på acceptabla villkor.

(27) I rekommendationen respekteras och iakttas de grundläggande rättigheterna och de vedertagna principer som erkänts bl.a. i Europeiska unionens stadga om de grundläggande rättigheterna. Särskilt syftar rekommendationen till att garantera full respekt för privatlivet och familjelivet samt skydd av personuppgifter.

([1]) EUT L 310, 9.11.2006, s. 15.
([2]) EUT L 412, 30.12.2006, s. 1.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

Syfte

1. I denna rekommendation ges riktlinjer till medlemsstaterna om utformningen och driften av RFID-tillämpningar på ett lagligt, etiskt och socialt och politiskt godtagbart sätt, med respekt för rätten till privatliv och garantier för skyddet av personuppgifter.

2. I denna rekommendation ges riktlinjer om de åtgärder som bör vidtas vid införande av RFID-tillämpningar för att se till att nationell lagstiftning för att genomföra direktiven 95/46/EG, 1999/5/EG och 2002/58/EG, i tillämpliga fall, följs när sådana tillämpningar införs.

Definitioner

3. Utöver de definitioner som anges i direktiv 95/46/EG avses i denna rekommendation med

a) *radiofrekvensidentifiering* (RFID)*:* användning av elektromagnetiska vågor eller induktiv koppling i radiofrekvensdelen av spektrumet för kommunikation till eller från en RFID-tagg med hjälp av en rad olika moduleringss- och kodningssystem i syfte att entydigt avläsa en RFID-taggs identitet eller andra uppgifter som lagrats på taggen,

b) *RFID-tagg* eller *tagg:* antingen en RFID-transponder som har förmåga att producera en radiosignal eller en RFID-transponder som kopplar om, återsprider eller reflekterar (beroende på typen av transponder) och modulerar en bärsignal som mottas från en läsare eller en skrivare,

c) *RFID-läsare* eller *RFID-skrivare eller läsare:* en fast eller rörlig anordning för datainsamling och identifiering med hjälp av radiofrekventa elektromagnetiska vågor eller induktiv koppling för att ge impuls till och skicka ett svar i form av modulerade data från en tagg eller en grupp av taggar,

d) *RFID-tillämpning* eller *tillämpning:* en tillämpning som behandlar uppgifter med hjälp av taggar och läsare, och som stöds av ett back-end-system och en nätbaserad kommunikationsinfrastruktur,

e) *operatör av RFID-tillämpning* eller *operatör:* en fysisk eller juridisk person, en myndighet, en byrå eller ett annat organ som, på egen hand eller tillsammans med andra, fastställer syftet med och medlen för driften av en tillämpning, inklusive registeransvariga som har ansvar för personuppgifter och som använder en RFID-tillämpning,

f) *informationssäkerhet:* bevarande av sekretess, integritet och tillgänglighet avseende information,

g) *övervakning:* alla verksamheter som genomförs för att upptäcka, observera, kopiera eller registrera en enskild persons vistelseort, rörelser, aktiviteter eller tillstånd.

Konsekvensanalyser avseende integritets- och dataskydd

4. Medlemsstaterna bör se till att branschen, i samarbete med berörda aktörer från det civila samhället, utarbetar en ram för konsekvensanalyser avseende integritets- och dataskydd. Denna ram bör läggas fram för godkännande av Artikel 29-arbetsgruppen inom 12 månader från offentliggörandet av denna rekommendation i *Europeiska unionens officiella tidning*.

5. Medlemsstaterna bör se till att operatörerna fullgör följande skyldigheter, oaktat deras andra skyldigheter enligt direktiv 95/46/EG:

a) Operatörerna ska genomföra en utvärdering av följderna av användningen av en tillämpning för skyddet av personuppgifter och integritetsskyddet, även när tillämpningen kan användas för att övervaka enskilda personer. Detaljnivån i utvärderingarna bör vara anpassad till de risker för integritetsskyddet som kan vara förknippade med tillämpningen i fråga.

b) Operatörerna ska vidta lämpliga tekniska och organisatoriska åtgärder för att garantera skyddet av personuppgifter och integritetsskyddet.

c) Operatörerna ska utse en person eller en grupp av personer som ansvarar för att se över utvärderingarna och bedöma om de tekniska och organisatoriska åtgärderna är fortsatt lämpliga för att garantera skyddet av personuppgifter och integritetsskyddet.

d) Operatörerna ska lämna in utvärderingarna till den behöriga myndigheten senast sex veckor innan RFID-tillämpningen ska börja användas.

e) Operatörerna ska genomföra ovannämnda bestämmelser i enlighet med den ram för konsekvensanalyser avseende integritets- och dataskydd som avses i punkt 4, så snart denna ram finns tillgänglig.

Informationssäkerhet

6. Medlemsstaterna bör stödja kommissionen i arbetet med att identifiera de RFID-tillämpningar som kan ge upphov till hot mot informationssäkerheten som kan få följder för allmänheten. För sådana tillämpningar bör medlemsstaterna garantera att operatörerna, tillsammans med de nationella behöriga myndigheterna och organisationer från det civila samhället, utarbetar nya system eller tillämpar befintliga system, såsom certifiering eller självanalyser av operatörerna, för att visa att nivån på informations- och integritetsskyddet är lämplig i förhållande till de utvärderade riskerna.

Information om och insyn i användningen av RFID

7. Utan att det påverkar de registeransvarigas skyldigheter i enlighet med direktiven 95/46/EG och 2002/58/EG ska medlemsstaterna se till att operatörerna utarbetar och offentliggör en kortfattad, korrekt och lättförståelig informationspolicy för var och en av sina tillämpningar. Policyn ska minst omfatta

a) operatörernas identitet och adress,

b) syftet med tillämpningen,

c) vilka uppgifter som ska behandlas av tillämpningen, särskilt om behandlingen omfattar personuppgifter, och om placeringen av taggarna kommer att övervakas,

d) en sammanfattning av konsekvensanalysen avseende integritets- och dataskyddet,

e) i förekommande fall, de sannolika riskerna för integritetsskyddet när det gäller användningen av taggarna i tillämpningen och de åtgärder som enskilda personer kan vidta för att minska dessa risker.

8. Medlemsstaterna bör se till att operatörerna vidtar åtgärder för att informera enskilda personer om förekomsten av läsare genom ett gemensamt EU-märke, som utvecklas av europeiska standardiseringsorganisationer med stöd av berörda intressenter. Märket bör innehålla information om operatörens identitet och uppgift om en kontaktpunkt där enskilda personer kan erhålla informationspolicyn för tillämpningen i fråga.

RFID-tillämpningar som används i detaljhandeln

9. Operatörerna bör, genom ett gemensamt EU-märke som tagits fram av europeiska standardiseringsorganisationer med stöd av berörda intressenter, informera enskilda personer om förekomsten av taggar som är placerade på eller inbyggda i produkter.

10. När operatören genomför den konsekvensanalys avseende integritets- och dataskyddet som avses i punkterna 4 and 5, bör operatören särskilt avgöra om taggar som placeras på eller byggs in i produkter som säljs till konsumenter genom detaljhandlare, som inte är operatörer för tillämpningen i fråga, utgör ett sannolikt hot mot privatlivet eller skyddet av personuppgifter.

11. Detaljhandlarna bör vid försäljningstillfället avaktivera eller avlägsna taggar som används i tillämpningar som de säljer om inte konsumenten, efter att ha informerats om den policy som avses i punkt 7, ger sitt godkännande till att taggarna ska fortsätta att vara operativa. Med avaktivering avses varje process som avbryter interaktionen mellan en tagg och dess omgivning och som inte kräver konsumentens aktiva inblandning. Avaktivering eller avlägsnande av taggar ska göras omedelbart och utan kostnad för konsumenterna. Konsumenterna ska kunna kontrollera att taggen verkligen har avaktiverats eller avlägsnats.

12. Punkt 11 gäller inte om man i konsekvensanalysen avseende integritets- och dataskyddet drar slutsatsen att taggar som används i en detaljhandelstillämpning, och som fortsätter att fungera även efter försäljningstillfället, inte utgör ett sannolikt hot mot skyddet av privatlivet eller personuppgifter. Detaljhandlarna ska emellertid kostnadsfritt tillhandahålla enkla hjälpmedel för att omedelbart eller i ett senare skede avaktivera eller avlägsna dessa taggar.

13. Avaktivering eller avlägsnande av taggar innebär inte att detaljhandlarens eller tillverkarens skyldigheter gentemot konsumenten på något sätt begränsas eller upphör.

14. Punkterna 11 och 12 gäller endast för detaljhandlare som är operatörer.

Informationskampanjer

15. Medlemsstaterna ska i samarbete med branschen, kommissionen och andra intressenter vidta lämpliga åtgärder för att informera och öka kunskapen bland myndigheter och företag, särskilt små och medelstora företag, om de möjliga fördelar och risker som är förknippade med användningen av RFID-teknik. Särskild uppmärksamhet bör ägnas åt informationssäkerhet och integritetsskydd.

16. Medlemsstaterna bör i samarbete med branschen, organisationer från det civila samhället, kommissionen och andra berörda intressenter identifiera och tillhandahålla exempel på god praxis i genomförandet av RFID-tillämpningar för att informera och öka kunskapen bland allmänheten. De bör även vidta lämpliga åtgärder, såsom storskaliga pilotprojekt, för att öka allmänhetens kunskap om RFID-teknik, om dess fördelar och risker samt om följderna av dess användning, som en nödvändig förutsättning för ett mer omfattande införande av denna teknik.

Forskning och utveckling

17. Medlemsstaterna bör samarbeta med branschen, relevanta intressenter från det civila samhället och kommissionen för att se till att principen ”security and privacy by design” introduceras redan i ett tidigt skede i utvecklingen av RFID-tillämpningar.

Uppföljning

18. Medlemsstaterna ska vidta alla nödvändiga åtgärder för att se till att alla intressenter som är involverade i utformningen och driften av RFID-tillämpningar inom gemenskapen får information om denna rekommendation.

19. Medlemsstaterna ska senast 24 månader efter offentliggörandet av denna rekommendation i *Europeiska unionens officiella tidning* meddela kommissionen vilka åtgärder som vidtagits för att följa rekommendationen.

20. Kommissionen ska inom tre år från offentliggörandet av denna rekommendation i *Europeiska unionens officiella tidning* lägga fram en rapport om genomförandet av rekommendationen, dess effektivitet och vilken inverkan den har haft på operatörer och konsumenter, särskilt när det gäller de åtgärder som rekommenderas i punkterna 9–14.

Adressater

21. Denna rekommendation riktar sig till medlemsstaterna.

Utfärdad i Bryssel den 12 maj 2009.

På kommissionens vägnar

Viviane REDING

Ledamot av kommissionen