

I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från europeiska datatillsynsmannen om meddelandet från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén "Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi" KOM(2007) 96

(2008/C 101/01)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av 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,

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41, och

AV FÖLJANDE SKÄL:

I. INLEDNING

1. Den 15 mars 2007 antog kommissionen ett meddelande om "Radiofrekvensidentifiering (RFID) i Europa: på väg mot en

strategi" ⁽¹⁾, (nedan kallat: *meddelandet*). Enligt artikel 41 i förordning (EG) nr 45/2001 är Europeiska datatillsynsmannen ansvarig för att ge råd till gemenskapsinstitutioner och gemenskapsorgan i alla frågor som rör behandling av personuppgifter. Europeiska datatillsynsmannen lägger fram detta yttrande i enlighet med denna artikel.

2. Detta yttrande ska ses som Europeiska datatillsynsmannens svar på meddelandet samt andra åtgärder på RFID-teknikens område som ägt rum sedan meddelandet antogs. De övriga åtgärder som beaktats i detta yttrande inkluderar:

— Kommissionens beslut av den 28 juni 2007 om upprättandet av en expertgrupp för radiofrekvensidentifiering ⁽²⁾ är en direkt följd av meddelandet. Denna grupp går också under namnet RFID-intressenterna. I enlighet med artikel 4.4 b i beslutet ska Europeiska datatillsynsmannen delta i gruppens arbete som observatör.

— Rådets resolution av den 22 mars 2007 om en strategi för ett säkert informationssamhälle i Europa ⁽³⁾.

— Projekt "RFID och identitetshantering", som Europaparlamentet tog initiativet till ⁽⁴⁾.

⁽¹⁾ KOM(2007) 96 slutlig.

⁽²⁾ Beslut nr 467/2007/EG (EUT L 176, 6.7.2007, s. 25).

⁽³⁾ EUT C 68, 24.3.2007, s. 1.

⁽⁴⁾ Projektet "RFID och identitetshantering – fallstudier om den mest avancerade utvecklingen när det gäller intelligent miljö (ambient intelligence)", beställt av Europaparlamentets STOA-panel (Scientific Technology Options Assessment) och utfört av ETAG (European Technology Assessment Group)
http://www.europarl.europa.eu/stoa/default_en.htm

- Antagande av artikel 29-arbetsgruppen för skydd av personuppgifter i juni 2007 av yttrande nr 4/2007 om begreppet personuppgifter ⁽¹⁾.
- Kommissionens meddelande till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet ⁽²⁾ och Europeiska datatillsynsmannens yttrande av den 25 juli 2007 om detta meddelande ⁽³⁾.
- Antagande av kommissionen av ett förslag till direktiv om ändring av (bland annat) direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation ⁽⁴⁾.
3. Europeiska datatillsynsmannen välkomnar kommissionens meddelande om RFID-tekniken, eftersom det tar upp de huvudfrågor som uppkommer i samband med spridningen av RFID-tekniken utan att försumma de avgörande frågor som hänför sig till skydd av personlig integritet och personuppgifter. Detta meddelande har dragit nytta av ett konsekvent och noggrant förberedelsearbete. Fem temainriktade arbetsmöten och ett offentligt samråd på Internet ⁽⁵⁾ på uppdrag av kommissionen har föregått detta meddelande.
4. Europeiska datatillsynsmannen instämmer i synpunkten att RFID-systemen kan komma att spela en avgörande roll i utvecklingen av informationssamhället, vilket man vanligen hänvisar till som "sakernas internet", och han delar helt de farhågor som nämns i punkt 3.2 i meddelandet för att RFID-system skulle kunna hota den enskildes rätt till skydd av personlig integritet och personuppgifter. Europeiska datatillsynsmannen har i sin årsrapport för 2005 identifierat RFID-tekniken tillsammans med system för biometrisk kännetecken, intelligent miljö och identitetshanteringssystem som en teknisk utveckling som kan förväntas få ett avgörande konsekvenser för skydd av personuppgifter.
5. Europeiska datatillsynsmannen finner att tillämpning av RFID-tekniken och dess acceptans i vida kretsar inte bara kommer att uppnås genom de tilltalande fördelar hos tekniken eller de nya tjänster den erbjuder, utan att den också kommer att underlättas genom fördelarna med väl utformade och stabila mekanismer för skydd av personuppgifter.
6. I korthet: Europeiska datatillsynsmannen karakteriserar RFID-tekniken som en i grunden ny teknisk utveckling, som i kommissionens meddelande med rätta betecknas som inkörsporten till en ny fas i utvecklingen av informations-samhället.
7. Denna utveckling väcker viktiga frågor på olika områden, varav ett är skydd av personlig integritet och personuppgifter. Detta yttrande från Europeiska datatillsynsmannen begränsar sig till detta område.

II. YTTRANDETS HUVUDSAKLIGA INRIKTNING

8. Detta yttrande inriktar sig särskilt på möjliga konsekvenser av denna utveckling när det gäller skydd av personlig integritet och personuppgifter. Dessa konsekvenser är för närvarande osäkra, vilket också beror på att utvecklingen av RFID-system och deras tillämpning är i full gång och att det inte på något sätt går att se vart denna utveckling kommer att leda.
9. Utifrån detta gör Europeiska datatillsynsmannen följande bedömning:
- För det första är det nödvändigt att klargöra de praktiska konsekvenserna av RFID-systemens spridning för skyddet av personlig integritet och personuppgifter.
 - För det andra är det nödvändigt att klargöra dessa konsekvenser i förhållande till den nuvarande rättsliga ramen för skyddet av personlig integritet och personuppgifter.
 - För det tredje tar Europeiska datatillsynsmannen upp frågan om huruvida dessa konsekvenser kräver mer specifika regler för frågor om skyddet av personlig integritet och personuppgifter som väckts genom användningen av RFID-teknik. Denna fråga togs redan upp av Europeiska datatillsynsmannen i dennes yttrande om meddelandet om dataskyddsdirektivet och kommer att utvecklas närmare i detta yttrande.
10. Genom att gå tillväga på detta sätt ämnar Europeiska datatillsynsmannen verka för att man vid utvecklingen och tillämpningen av RFID-system tar berättigad hänsyn till skyddet av personlig integritet och personuppgifter.

III. KLARGÖRANDE AV KONSEKVENSERNA

RFID-system och RFID-etiketter

11. Trots att – som sagts ovan – utvecklingen är i full gång och resultatet är osäkert, är det helt möjligt att beskriva de huvudsakliga kännetecknen för utvecklingen med hänsyn till konsekvenserna för skyddet av personuppgifter.

⁽¹⁾ Dokument WP 136, som är offentliggjort på arbetsgruppens webbplats.

⁽²⁾ Kommissionens meddelande av den 7 mars 2007 från kommissionen till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, KOM(2007) 87 slutlig.

⁽³⁾ EUT C 255, 27.10.2007, s. 1, om "Yttrande om meddelandet om dataskyddsdirektivet".

⁽⁴⁾ Förslag till Europaparlamentets och rådets direktiv av den 13 november 2007 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskydds-samarbete, KOM(2007) 698 slutlig. Hänvisning till direktiv 2002/58/EG kommer att göras med "direktivet om integritetsskydd och elektronisk kommunikation".

⁽⁵⁾ <http://www.rfidconsultation.eu/>

12. Vid bedömningen av de aspekter i RFID-tekniken som har potentiella följder för skydd av personlig integritet och personuppgifter är det mycket lämpligt att inte bara beakta RFID-etiketterna utan också RFID-teknikens hela bakomliggande uppbyggnad: etikett, läsare, nätverk, referensdatabas och den databas där de personuppgifter vilka tagits fram genom att förbinda etikett och läsare är lagrade. Så som det i korthet framhåvs i inledningen i meddelandet, handlar RFID inte bara om "elektroniska etiketter", varför frågor om skyddet av personuppgifter inte enbart kommer att begränsas till etiketter utan utvidgas till delar av RFID-teknikens bakomliggande uppbyggnad. Var och en av dessa element har en uppgift när det gäller att vid behov bidra till genomförandet av en rättslig ram för EU:s skydd av personuppgifter. De kommer att styras av de huvudsakliga trenderna inom ramen för utvecklingen av informationssamhället, som en nästan obegränsad bandbredd, allmänt utbredda nätverksanslutningar och en oändlig lagringskapacitet.

Effekten av RFID-system och RFID-etiketter

13. Trots behovet av ett vidare synsätt, som framhölls i föregående stycke, finns det flera olika skäl som gör det berättigat att i första hand koncentrera sig på användningen av RFID-tekniken när det gäller etikettering av konsumentprodukter inom detaljhandelssektorn. Det självklara skälet är den förväntade utökade användningen av tekniken, som tycks utvecklas mot en mycket utbredd tillämpning. I motsats till andra RFID-tillämpningar med en snäv eller begränsad användning, har etikettering på artikelnivå den största potentiella möjligheten att bli en tillämpning för massmarknaden. Många konsumentprodukter är redan nu försedda med en RFID-etikett. I koppling till detta är förhållandet att denna typ av användning kommer att påverka ett stort antal enskilda personer vilkas personuppgifter förmodligen kommer att behandlas varje gång dessa individer inhandlar en produkt med en infogad RFID-etikett.

14. Särskild uppmärksamhet måste ägnas åt de konsekvenser som RFID-etiketteringen av artiklar får för deras ägare. RFID-systemen skulle kunna tänja ut förhållandet mellan en artikel och dess ägare. När en gång detta förhållande har tänjts ut, kan ägaren bli skannad och klassificerad som "lågbudget" eller som en person som tillhör en "attraktiv målgrupp" för framtida transaktioner; överdriven personlig bearbetning (one-to-one) ⁽¹⁾ kan leda till att vissa beteenden automatiskt "bestraffas" (kräva återvinning, sophantering osv.). Enskilda personer bör inte utsättas för ett förfarande där ogynnsamma beslut fattas automatiskt. Genom katalyseringsförmågan hos denna RFID-teknik ökar risken för att informationssamhället närmar sig en situation där det kommer att fattas automatiska beslut och där tekniken kommer att missbrukas för att styra det mänskliga beteendet.

15. De uppgifter som finns lagrade i eller är framtagna genom en RFID-etikett kan utgöras av personuppgifter enligt definitionen i artikel 2 i dataskyddsdirektivet. Som exempel kan

smartkort som används vid resa innehålla vissa uppgifter för identifiering och uppgifter om kortinnehavarens nyligen gjorda resor. Om en skrupelfri person skulle vilja spåra enskilda personer, skulle det räcka med att strategiskt placera ut läsare som tillhandahåller uppgifter om kortinnehavarens förflyttningar och på detta sätt inkräkta på dessa personers integritet och personuppgifter.

16. Liknade hot mot den personliga integriteten skulle kunna uppkomma även om den lagrade informationen på RFID-etiketten inte skulle innehålla uppgifter om individernas namn. RFID-etiketter innehåller en unik identifiering kopplad till konsumentprodukter: om varje etikett har en unik identitet, kan denna identifiering användas i bevakningssyfte. Om en person har på sig en klocka med en RFID-etikett med ett ID-nummer, kan exempelvis detta nummer tjäna som en unik identifiering av personen som bär denna klocka, även om personens identitet inte är känd. Det sätt på vilket dessa uppgifter används – och hur de sätts i relation till själva klockan eller individen ifråga – avgör om direktivet kan tillämpas eller inte. Direktivet skulle exempelvis tillämpas om information genereras om var personen befinner sig och detta sannolikt kommer att användas för att övervaka dennes beteende eller för pris-differentiering, för att neka tillträde eller för icke-önskad reklam.

17. I detta sammanhang är det nödvändigt att säkerställa att RFID-tillämpningar utvecklas med nödvändiga tekniska åtgärder för minimera risken för ofrivilligt röjande av personuppgifter. Sådana åtgärder kan innehålla ett krav på att den bakomliggande uppbyggnaden av RFID-tekniken och särskilt att RFID-etiketterna utformas på ett sådant sätt att ett sådant resultat förhindras. RFID-etiketter kan exempelvis distribueras med ett inaktiveringskommando (kill command) som gör det möjligt att inaktivera dem. Denna möjlighet kommer att diskuteras ytterligare i avsnitt IV i yttrandet.

18. Genom att erbjuda möjligheten att spåra artiklar sedan de lämnat försäljningsstället, inför RFID-systemen nya frågeställningar i debatten om personlig integritet. Två aspekter kommer att behöva beaktas när effekten analyseras hur pass kopplad till personen anses artikeln vara och hur lättroblig är den ⁽²⁾?

19. Livscykeln för en artikel kan också vara ett komplement till den riskanalys som krävs och kan bidra till den kvantitativa bedömningen av de potentiella hoten mot den personliga integriteten. Med tanke på att en RFID-etikett kanske inte inaktiveras, skulle en slutanvändarprodukt med en lång livscykel kunna samla ytterligare närliggande personuppgifter om artikelns ägare och bygga upp en noggrannare personbeskrivning. På andra sidan kan en kort livscykel hos en artikel, som exempelvis en burk läsk, från tidpunkt för tillverkning till återvinning innebära mindre risk och den skulle därför kunna kräva lindrigare åtgärder än en produkt men en betydligt längre livscykel.

⁽¹⁾ Dr. Sarah Spiekerman, chef för Berlin Research Centre on Internet Economics, workshop om "RFID and ubiquitous computing" organiserad av Trans Atlantic Consumer Dialogue den 13 mars 2007.

⁽²⁾ Dara J. Glasser, Kenneth W. Goodman och Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volym 9, nr 2, 2007.

Skydd av personlig integritet och personuppgifter vid utveckling av RFID-system

20. För att bättre förstå de följderna som RFID-systemen får för skyddet av personlig integritet och personuppgifter kan fem grundläggande frågeställningar urskiljas när det gäller skydd för personlig integritet och personuppgifter.
21. Den första frågan gäller identifiering av den registrerade personen. För mer än 60 år sedan var syftet med en RFID-etikett att identifiera om det var en vän eller fiende som närmade sig. Idag kan RFID-systemen inte bara identifiera de allmänna beståndsdelarna i ett föremål utan de kommer i slutändan att kunna leda till identifiering av en enskild person och de behöver därför göra det på ett sätt som främjar skyddet av personuppgifter.
22. Den andra frågan gäller identifiering av den registeransvarige personen. När det gäller RFID-system, kan identifieringen av den registeransvarige enligt definitionen i artikel 2 d i dataskyddsdirektivet vara svårare att göra, varför det behövs en grundligare granskning. Identifieringen av den registeransvarige är emellertid fortfarande ett viktigt steg när det gäller att fastställa ansvaret för var och en av de berörda aktörer som måste rätta sig efter den rättsliga ramen för skyddet av personuppgifter. Under RFID-etikettens livscykel kan den registeransvarige som hanterar uppgifterna skifta flera gånger på grund av de tilläggs-tjänster som kan erbjudas kopplade till det etiketterade föremålet.
23. Den tredje frågan gäller den minskade innebörden av den traditionella åtskillnaden mellan den privata och den offentliga sfären. Även om åtskillnaden mellan den privata och den offentliga sfären också förr i världen inte alltid var entydig, är de flesta människor medvetna om gränserna mellan dem (och om gråzonerna) och de fattar initierade eller intuitiva beslut om hur de ska agera därefter. Enligt Hall ⁽¹⁾ uppfattas det personliga utrymmet vanligen som det fysiska avståndet till andra personer. Hanteringen av den personliga sfären kan också ses som en dynamisk gränsdragningsprocess ⁽²⁾. Det är därför inte förvånande att den trådlösa kommunikationen med RFID-etiketten samt förmågan till icke synlig avläsning väcker oro genom att den traditionella gränsdragningen suddas ut. Det finns förvisso en rädsla för att den enskilda personen helt eller delvis kan förlora kontrollen över det personliga utrymme som han eller hon tidigare haft. Därför har både de som talar för och de som talar emot systemet riktat in sig på avläsningsavståndet i de första tillämpningarna av RFID-systemen.
24. Den fjärde frågan handlar om hur man ska hantera RFID-etikettens storlek och fysiska egenskaper. Eftersom etiketten i grunden måste vara liten billig, kommer de säkerhetsåtgärder som kan utvecklas för denna del av RFID-systemet per definition att vara begränsade. Kommunikationens trådlösa natur lägger emellertid till en ytterligare risknivå i jämförelse med trådbunden kommunikation, varför det behövs ytterligare säkerhetsåtgärder.
25. Den femte frågan är bristen på insyn vid hanteringen. RFID-system kan leda till insamling och bearbetning av uppgifter som kan användas för att kartlägga en person utan att det upptäcks. Denna konsekvens kan mycket väl illustreras genom att jämföra RFID-system med mobiltelefonen, vilket är något som görs allt oftare. På ena sidan drog mobiltelefonen nytta av en mycket hög acceptansnivå när det gäller teknik oberoende av den potentiella risken för intrång i den personliga integriteten. Man skulle kunna dra slutsatsen att RFID-tekniken kommer att accepteras på samma sätt. På andra sidan måste man framhålla att en mobiltelefon är ett synligt föremål som fortfarande kontrolleras av den slutliga användaren, eftersom den kan stängas av. Detta förhållande gäller inte för RFID-tekniken.
26. Även om den omärkliga insamlingen och hanteringen av personuppgifter enligt ovan kan vara laglig, är det också möjligt och under olika omständigheter till och med ganska sannolikt att det sker en olaglig insamling och hantering av sådana uppgifter.
27. Klargörandena i detta avsnitt motiverar följande slutsatser. Den utbredda användningen av RFID-tekniken är något i grunden nytt och kan få en avgörande inverkan på vårt samhälle och skyddet av grundläggande rättigheter i vårt samhälle såsom personlig integritet och skydd av personuppgifter. RFID-tekniken kan leda till en kvalitativ förändring.

IV. PRECISERING AV KONSEKVENSERNA

Inledning

28. Detta avsnitt kommer huvudsakligen att inrikta sig på RFID-teknikens inverkan på de grundläggande rättigheterna i vårt samhälle, så som skydd av personlig integritet och personuppgifter. Dessa effekter kommer att anges i två steg, den första är en kort beskrivning av hur de grundläggande rättigheter skyddas inom ramen för den nuvarande rättsliga ramen. I ett andra steg kommer Europeiska datatillsynsmannen att närmare utveckla möjligheterna att till fullo utnyttja den nuvarande rättsliga ramen. Denna ambition var införd i yttrandet om meddelandet om dataskyddsdirektivet som "fullständigt genomförande av direktivets nuvarande bestämmelser".
29. Utgångspunkten är följande: Utveckling av ny teknik som RFID-systemen har en klar inverkan på kraven på en effektiv rättslig ram för skydd av personuppgifter. Dessutom kan behovet av ett effektivt skydd av en enskilds personuppgifter medföra begränsningar för användningen av den nya tekniken. Samspelet verkar således i båda riktningar: Tekniken påverkar lagstiftningen och lagstiftningen påverkar tekniken ⁽³⁾.

⁽¹⁾ Edward T. Hall, 1966, *The Hidden Dimension* (1:a upplagan), Garden City, N.Y.: Doubleday.

⁽²⁾ Altman I. 1975, *The Environment and Social Behaviour*, Brooks/Cole Monterey.

⁽³⁾ Se europeiska datatillsynsmannens yttrande från mars 2006 om kommissionens meddelande om interoperabilitet mellan europeiska databaser, offentliggjort på Europeiska datatillsynsmannens webbplats.

Skydd av grundläggande rättigheter

30. Skyddet av den grundläggande rätten till personlig integritet och skydd av personuppgifter inom Europeiska unionen garanteras i första hand genom en rättslig ram, vilket är nödvändigt, eftersom det handlar om rättigheter som är erkända i artikel 8 i den Europeiska konventionen om mänskliga rättigheter och grundläggande friheter och i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Den relevanta rättsliga ramen för skydd av personuppgifter och RFID-tekniken utgörs av dataskyddsdirektivet 95/46/EG och direktivet om integritet och elektronisk kommunikation 2002/58/EG ⁽¹⁾.
31. Den generella rättsliga ramen för skydd av personuppgifter i enlighet med direktiv 95/46/EG gäller RFID-tekniken i den utsträckning som de uppgifter som hanteras av RFID-system omfattas av definitionen för personuppgifter. Medan det i vissa fall står helt klart att RFID-tillämpningar hanterar personuppgifter och utan tvivel omfattas av dataskyddsdirektivet, finns det också tillämpningar där det inte är så uppenbart att dataskyddsdirektivet ska tillämpas. Yttrande nr 4/2007 från artikel 29-arbetsgruppen för skydd av personuppgifter om begreppet "personuppgifter" syftar till att bidra till en klarare och allmänt erkänd tolkning av begreppet personuppgifter och på så sätt minska denna osäkerhet ⁽²⁾.
32. När det gäller direktivet om integritet och elektronisk kommunikation, råder följande situation: Det är ännu inte klart om detta direktiv ska gälla RFID-tillämpningar. Kommissionens förslag av den 13 november 2007 om ändring av direktivet innehåller därför en bestämmelse med syfte att fastställa att direktivet förvisso gäller vissa RFID-tillämpningar. Men andra RFID-tillämpningar omfattas eventuellt inte, på grund av att tillämpningen av detta direktiv är begränsad till behandling av personuppgifter i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät.
33. Skyddet av personuppgifter kan kompletteras med en rad självreglerande instrument (icke-lagstiftningsram). Användning av dessa instrument stöds aktivt i de båda direktiven, särskilt i artikel 27 i dataskyddsdirektivet som föreskriver att medlemsstaterna och kommissionen ska uppmuntra utarbetande av uppförandekodexar som ska bidra till ett korrekt genomförande av direktivet. Dessutom kan självreglerande instrument effektivt bidra till genomförandet att kraven på säkerhetsåtgärder i artikel 17 i dataskyddsdirektivet och artikel 14 i direktivet om integritet och elektronisk kommunikation.

⁽¹⁾ Punkt 59 i detta yttrande kommer att ta upp tillämpligheten av ett tredje direktiv, nämligen Europaparlamentets och rådets direktiv 1999/5/EG av den 9 mars 1999 om radioutrustning och teleterminalutrustning och om ett ömsesidigt erkännande av utrustningens överensstämmelse (EGT L 91, 7.4.1999, s. 10).

⁽²⁾ Se bland annat s. 10 i yttrandet, som åberopas i fotnot nr 5.

Fullständig tillämpning av den gällande rättsliga ramen

34. Yttrandet om meddelandet om dataskyddsdirektivet innehåller en förteckning över tillgängliga instrument för en bättre tillämpning av direktivet. De flesta icke-bindande instrumenten i detta yttrande är tillämpliga när det gäller RFID-tekniken, som exempelvis tolkningsmeddelanden eller andra meddelanden, främjande av bästa metoder, användande av integritetsmärkning och granskning av tredje part. Möjligheten att anta särskilda regler för RFID-tekniken kommer att tas upp i avsnitt V. Men förbättringar är också möjliga inom den nuvarande rättsliga ramen.

Självreglerande instrument

35. Europeiska datatillsynsmannen är överens med kommissionen om att det i ett första steg är lämpligt att lämna utrymme för självreglering, vilket ger de berörda parterna möjlighet att snabbt inrätta en miljö som uppfyller de rättsliga kraven och på så sätt skapar ett säkrare rättsläge.
36. Kommissionen förväntas i samråd med RFID-intressenterna stimulera och styra denna självregleringsprocess. I samband härmed välkomnar Europeiska datatillsynsmannen den rekommendation som aviseras i meddelandet och som förväntas innehålla specifika riktlinjer för att fastställa "de principer som myndigheterna och andra intressenter bör tillämpa när det gäller RFID-användning".
37. Enligt meddelandet ska självregleringen utformas som en uppförandekod eller som riktlinjer för god praxis. Enligt Europeiska datatillsynsmannen bör självregleringen oberoende av vilken form den får
- ge konkreta och praktiska riktlinjer för specifika typer av RFID-tillämpningar och på så sätt bidra till efterlevnad av den rättsliga ramen för skydd av personuppgifter,
 - åtgärda de specifika frågor som rör skyddet av personuppgifter och de problem som uppstår i samband med generiska RFID-tillämpningar,
 - bidra till en enhetlig och harmoniserad tillämpning av dataskyddsdirektivet i hela EU, i synnerhet inom en sektor som sannolikt kommer att använda samma typ av RFID-tillämpningar inom hela EU,
 - tillämpas av samtliga berörda intressenter. Bristande efterlevnad bör få negativa följder (möjlig ekonomiska).

38. Europeiska datatillsynsmannen pekar på ett område där självreglering kommer att vara särskilt användbar. För de RFID-tillämpningar som är förenade med hantering av personuppgifter ålägger dataskyddsdirektivet de registeransvariga olika skyldigheter, särskilt enligt artikel 17 (säkerhet vid behandling) och enligt artikel 7 (personuppgifter får behandlas endast om det föreligger en tillämplig rättslig grund). I enlighet med dessa bestämmelser måste de registeransvariga på ena sidan vidta åtgärder mot en otillåten spridning av personuppgifter. På andra sidan måste de registeransvariga säkerställa att behandlingen, såsom spridning av information genom läsare, i förekommande fall, endast sker med informerat samtycke från den person som personuppgifterna hänför sig till.
39. Dessa bestämmelser i dataskyddsdirektivet kan tolkas som ett krav på att RFID-tillämpningar ska utvecklas med nödvändiga tekniska lösningar för att förhindra eller minimera riskerna för oönskad spridning och säkerställa att behandling eller överföring av uppgifter endast sker med informerat samtycke i förekommande fall. Europeiska datatillsynsmannen anser att ett sådant krav (dvs. att tillämpa nödvändiga tekniska lösningar för att minimera riskerna för oönskad spridning) och dess bindande art för dem som utvecklar RFID-tillämpningar, kommer att vara ännu starkare och tydligare om detta krav tas med i den kommande uppförandekoden eller i riktlinjerna för god praxis, enligt ovan. Av dessa skäl förordar Europeiska datatillsynsmannen starkt att det i kommissionens rekommendation inkluderas en sådan tolkning av dataskyddsdirektivet och att det betonas att det finns en skyldighet att utveckla RFID-tillämpningar försedda med nödvändiga tekniska åtgärder för att förhindra oönskad insamling eller spridning av personuppgifter.
- Behovet av riktlinjer**
40. Europeiska datatillsynsmannen rekommenderar kommissionen att i nära samarbete med expertgruppen för RFID-teknik ta fram en eller flera dokument som ger en klar ledning om hur den nuvarande rättsliga ramen ska gälla för RFID-miljön. Vägledningen bör ange praktiska sätt för hur efterlevnad av principerna i dataskyddsdirektivet och i direktivet om integritet och elektronisk kommunikation ska ske. När det gäller det övergripande synsättet i vägledningen och dess konkreta innehåll, har Europeiska datatillsynsmannen följande förslag:
41. Vägledningen med de principer som gäller RFID-användning bör vara tillräckligt fokuserad och införa ett synsätt som är specifikt för detta område. En standardlösning kommer inte att förverkliga det eftersökta syftet att säkerställa en klar och enhetlig ram. Vägledningens räckvidd måste i stället begränsas till väl definierade tillämpningar på RFID-området.
42. Dessutom bör riktlinjerna föreslå praktiska och effektiva metoder för att utveckla metoder och normer som kan bidra till att RFID-systemen uppfyller bestämmelserna i den rättsliga ramen för skydd av personuppgifter och kommer att medföra användande av en teknik med inbyggda skyddsmekanismer för den personliga integriteten (privacy by design).
43. Vid tillämpning av den gällande rättsliga ramen på RFID-miljön måste särskild uppmärksamhet ägnas tillämpningen av principerna om skydd för den personliga integriteten och de skyldigheter som åligger registeransvariga för RFID-tillämpningar. Särskilt relevanta är följande skyldigheter och principer:
- Principen om rätt till information, inklusive rätten att få veta när uppgifter samlas in med hjälp av läsare och i relevanta fall när produkter är försedda med RFID-etiketter.
 - Samtycke som en av de juridiska grunderna för behandling av personuppgifter. Detta begrepp materialiseras i skyldigheten att inaktivera RFID-etiketterna vid försäljningsstället, om inte den person som uppgifterna gäller givit sitt samtycke (!). Rätten att få RFID-etiketterna inaktiverade tjänar också syftet att säkerställa skydd för informationen, dvs. säkerställa att de uppgifter som behandlas genom RFID-etiketter inte sprids till en icke önskad tredje part.
 - Den enskildes rätt att inte utsättas för ogynnsamma beslut som enbart baseras på den automatiserade behandlingen av en fastställd personlig profil.
44. När det gäller rätt till information, bör vägledningen fastställa att enskilda personer måste erhålla information om behandlingen av deras personuppgifter. De bör i synnerhet bland annat underrättas om att i) det finns läsare och aktiverade RFID-etiketter på produkter och deras förpackningar, ii) följderna av denna förekomst när det gäller insamling av information och iii) det avsedda syftet med insamlingen av information.
45. Det kan vara lämpligt att använda logotyper som en åtgärd för att ge information. Logotyper kan användas för att underrätta om förekomsten av läsare och RFID-etiketter som förväntas vara aktiva. Enbart användningen av logotyper kommer emellertid inte att räcka för att säkerställa en korrekt behandling av information, vilket kräver att informationen lämnas till den person som uppgifterna gäller på ett klart och begripligt sätt. Användningen av logotyper bör anses som en kompletterande åtgärd till bestämmelsen om mer detaljerad information.

(!) Se mer i detalj punkt 46–50 i detta yttrande.

Grundvalen: Principen om frivilligt deltagande

46. För samtliga berörda RFID-tillämpningar bör lösningarna som en förutsättning respektera och tillämpa principen om frivilligt deltagande vid försäljningsstället. Att möjliggöra för RFID-etiketterna att fortsätta att sända information efter försäljningen vore olagligt, om inte den registeransvarige har rättsliga grunder. Tillämpliga rättsliga grunder vore i normalfallet enbart a) samtycke av den person som uppgifterna gäller eller b) en särskild och frivillig begäran av denna enskilda person, om en sådan spridning är nödvändig för att tillhandahålla en tjänst⁽¹⁾. De båda rättsliga grunderna ska då betecknas som frivilligt deltagande.
47. Enligt principen om frivilligt deltagande bör RFID-etiketterna inaktiveras vid försäljningen, om inte den enskilde som köpt artikeln med vidhängande etikett vill att den lämnas aktiv. Genom att utnyttja rätten att låta etiketten förbli aktiv, skulle den enskilde ge sitt samtycke till ytterligare behandling av hans eller hennes personuppgifter, exempelvis överföring av uppgifterna till läsaren vid nästa besök hos den registeransvarige.
48. För att klara av den ökande mångfalden av RFID-tillämpningar och underlätta utvecklingen av nya innovativa företagsmodeller, understryker Europeiska datatillsynsmannen vikten av en flexibel strategi. Flexibilitet måste erbjudas vid tillämpning av frivillighetsprincipen.
49. Alternativen till tillämpning av frivillighetsprincipen är av många slag. Exempelvis skulle man som ett alternativ till att avlägsna etiketten kunna tänka sig att etiketten blockeras, tillfälligt inaktiveras eller enligt en säkerhetsmodell som går under namnet *den återupståndna ankungen*⁽²⁾ binds till en särskild användare. När det gäller en etikett med kort livslängd, skulle också den på etiketten angivna adressen, som noggrant anger information som är lagrad i en databas, kunna raderas från referensdatabasen, varvid vidare behandling av ytterligare uppgifter som samlas in genom etiketten skulle undvikas.
50. Sammanfattningsvis, även om Europeiska datatillsynsmannen anför skäl för att principen om frivilligt deltagande vid försäljningsstället är en juridisk skyldighet som i de flesta fall redan är i kraft enligt dataskyddsdirektivet, finns det goda skäl att klart ange denna skyldighet i självreglerande instrument, vilket också gäller för att säkerställa att principen kommer att tillämpas på det mest ändamålsenliga sättet. Särskild tillämpning är under alla förhållanden nödvändig för de RFID-tillämpningar som inte omfattas av dataskyddsdirektivet.

(1) När det gäller vissa RFID-tillämpningar, kan det eventuellt vara möjligt att stödja sig på andra grunder, som exempelvis artikel 7 f (berättigade intressen hos den registeransvarige, under förutsättning av tillräckliga skyddsåtgärder).

(2) Namnet på denna modell som utvecklats av Frank Stajano och Ross Anderson på universitetet i Cambridge, är inspirerat av att "en ankunge som kommer ut ur sitt ägg uppfattar det första levande objekt den ser som sin mor".

Behovet av inbyggda skyddsmekanismer för att skydda den personliga integriteten (privacy by design)

51. För att minimera hoten mot skyddet för personlig integritet och personuppgifter, stöds i kommissionens meddelande i avsnitt 3.2 på sidan 6 idén om att utarbeta specifikationer och anta konstruktionskriterier på ett tidigt stadium. Europeiska datatillsynsmannen välkomnar detta synsätt. Antagandet av specifikationer och konstruktionskriterier, även kallat "bästa tillgängliga teknik" (BAT), kommer förvisso att effektivt bidra till efterlevnaden av dataskyddsförordningen och säkerhetskrav. Denna identifiering av tekniska och organisatoriska kriterier kommer, om den ses över ofta, att stärka den modell för symbios mellan integritets- och säkerhetskrav som Europeiska unionen håller på att utveckla.
52. En fullgod definition av BAT för personlig integritet och skydd av personuppgifter för RFID-system kommer också att vara avgörande för att bygga upp en förtroendeingivande miljö som kommer att förstärka en utbredd acceptans bland de slutliga användarna samt för den europeiska industrins konkurrenskraft.
53. Förfarandet för att välja ut bästa tekniska lösningar för RFID-system bör få stöd av konsekvensbedömningar för personlig integritet och skydd för personuppgifter, vilka man fortfarande behöver satsa på. Europeiska datatillsynsmannen anser att Europeiska byrån för nät- och informationssäkerhet och Europeiska kommissionens gemensamma forskningscentrum tillsammans med berörda intressenter inom industrin kan bidra till identifiering av bästa tillgängliga teknik och utveckling av sådana metoder. Genom att nyligen lansera projektet "Technische Richtlinien für den sicheren RFID-Einsatz" (Tekniska riktlinjer för säker användning av RFID-tekniken) gav det tyska förbundsorganet *Bundesamt für Sicherheit in der Informationstechnik* (BSI) ett passande och illustrativt exempel⁽³⁾ på den bästa tillgängliga teknik som nu bör utvecklas på europeisk nivå.
54. Normer kan också spela en avgörande roll för att principen om inbyggda skyddsmekanismer som skydd för den personliga integriteten vid produktens utformning antas på ett tidigt stadium. Kommissionen bör därför bidra till man antar skyddsåtgärder för personlig integritet och personuppgifter vid utvecklingen av internationella normer för RFID-tekniken. Artikel 29-arbetsgruppen har i sitt arbetsdokument⁽⁴⁾ om RFID-tekniken klart illustrerat möjligheten av att normer kan bidra till utvecklingen av RFID-system som går väl ihop med den personliga integriteten.

(3) <http://www.bsi.bund.de/veranst/rfid/index.htm>

(4) Arbetsdokument (WP 105) om frågor som avser skydd av personuppgifter i samband med RFID-teknik av den 19 januari 2005.

55. Europeiska datatillsynsmannen välkomnar dessutom den ståndpunkt som kommissionen antagit när det gäller forskning och utveckling avseende RFID-tekniken samt behovet av att minska riskerna för den personliga integriteten. Principen om inbyggda skyddsmekanismer för skydd av den personliga integriteten vid produktutformningen behöver förvisso införas så tidigt som möjligt i utvecklingen av tekniken, något som på ett bättre sätt bidrar till deras överensstämmelse med den rättsliga ramen för skydd av personuppgifter. Europeiska datatillsynsmannen kommer som kort anges i årsrapporten för 2006 att stödja denna strävan genom att från fall till fall lämna yttranden och råd om projekt inom 7:e ramprogrammet (2007-2013).

V. BEHÖVS DET SÄRSKILDA LAGSTIFTNINGSAÅTGÄRDER?

56. Självreglering är kanske inte tillräckligt för en full tillämpning av den nu gällande rättsliga ramen för skydd av personlig integritet och personuppgifter. Även om självreglering uppfyller de ovan nämnda kraven, är tillämpningen frivillig och påföljder för att kraven inte efterlevs kan inte alltid ges på ett effektivt sätt. Dessutom kan bindande rättsliga åtgärder fortfarande behövas för att säkerställa den enskildes rätt till skydd av personlig integritet och personuppgifter. Behovet är ännu större när det självreglerande förfarandet misslyckas.

57. En avgörande fråga är vilka rättsliga instrument som behövs för att säkerställa att RFID-tillämpningarna faktiskt utvecklas med de nödvändiga tekniska lösningarna för att förhindra eller minimera riskerna för skyddet av personlig integritet och personuppgifter och att de registeransvariga vidtar adekvata åtgärder för efterlevnad av sina skyldigheter enligt den gällande rättsliga ramen. Detta ger upphov till några ytterligare frågor:

— Behövs det särskilda regler?

— Om så är fallet, kan dessa regler antas inom den gällande rättsliga ramen, exempelvis genom att använda nuvarande kommittéförfaranden?

— Är det nödvändigt med ett nytt rättsligt instrument för att säkerställa en effektiv utveckling av RFID-tillämpningar med inbyggd teknik för förbättrat skydd av den personliga integriteten?

58. Detta avsnitt kommer att behandla möjligheterna av att införa bindande rättsliga åtgärder inom den gällande rättsliga ramen, medan avsnitt VI diskuterar behovet av ett nytt rättsligt instrument, eftersom det är en separat fråga.

59. För det första bör särskild uppmärksamhet ägnas åt bestämmelserna i artikel 17 i direktiv 95/46/EG, artikel 14.3 i direktiv 2002/58/EG och artikel 3.3 c i direktiv 1999/5/EG. I enlighet med artikel 14.3 kan medlemsstaterna vidta åtgärder för att säkerställa att terminalutrustning är så konstruerad att den är förenlig med användarnas rätt till skydd och kontroll av sina personuppgifter i enlighet med

direktiv 1999/5/EG⁽¹⁾. I artikel 3.3 c i direktiv 1999/5/EG föreskrivs det att kommissionen, med ett kommittéförfarande, får besluta att utrustning i vissa utrustningsklasser eller viss slags utrustning ska vara så konstruerad att den innehåller skyddsmekanismer för att säkerställa att användarens och abonnentens personuppgifter och privatliv skyddas. Bestämmelserna i artikel 3.3 c i direktiv 1999/5/EG har ännu inte kommit till användning.

60. Dessa bestämmelser ger lagstiftaren, på nationell och på gemenskapsnivå, befogenhet att föreskriva att skyddsmekanismer för den personliga integriteten måste inkluderas vid konstruktionen av RFID-system, vilket är ett koncept som går under namnet "privacy by design"⁽²⁾. Det krävs också att bästa tillgängliga teknik används.

61. För att användningen av konceptet inbyggda skyddsmekanismer för den personliga integriteten (privacy by design) ska bli obligatorisk, rekommenderar Europeiska datatillsynsmannen att kommissionen använder sig av mekanismen i artikel 3.3 c i direktiv 1999/5/EG i samråd med expertgruppen för RFID-tekniken.

62. För det andra är det möjligt att specificera tillämpningen av den nu rådande rättsliga ramen på RFID-tekniken genom en ändring dessa direktiv. Som tidigare sagts har kommissionen just lagt fram ett förslag till ändring av direktivet om integritet och elektronisk kommunikation med en ny bestämmelse med detta syfte. Europeiska datatillsynsmannen välkomnar denna första bekräftelse på att detta direktiv kan tillämpas på RFID-tillämpningar. Europeiska datatillsynsmannen kommer att behandla särskilda frågor i samband med förhållandet mellan direktivet om integritet och elektronisk kommunikation och RFID-tekniken i sitt yttrande om förslaget till ändring, vilket kommer att läggas fram i början av 2008.

63. Med beaktande av att kommissionen inte planerar någon ändring av dataskyddsdirektivet inom den närmaste framtiden⁽³⁾ är möjligheterna till en specificering av tillämpningen av den nu gällande rättsliga ramen på RFID-tekniken begränsad.

VI. BEHÖVS DET EN SÄRSKILD RÄTTSLIG RAM FÖR RFID-TEKNIKEN?

Kommissionens avsikter

64. Meddelandet⁽⁴⁾ understryker vikten av säkerhet och inbyggda skyddsmekanismer för personlig integritet (privacy by design) Det krävs också deltagande av samtliga intressenter. Det huvudsakliga resultatet av kommissionens

⁽¹⁾ I enlighet med rådets beslut 87/95/EEG av den 22 december 1986 om standardisering inom området informationsteknologi och telekommunikation (EGT L 36, 7.2.1987, s. 31).

⁽²⁾ Se avsnitt IV.

⁽³⁾ Europeiska datatillsynsmannen stöder denna ståndpunkt, se punkt 64.

⁽⁴⁾ Se punkt 4.1 i meddelandet.

insatser kommer att bli "en rekommendation för att fastställa de principer som myndigheterna och andra intressenter bör tillämpa när det gäller RFID-användning". Rekommendationen kommer troligen att antas under våren 2008. Ambitionerna med avseende på lagstiftningen är i meddelandet uppdelade i två steg. Kommissionen kommer att

— överväga lämpliga bestämmelser avseende RFID-tekniken i det kommande förslaget till ändring av direktivet om integritet och elektronisk kommunikation. Som tidigare sagts lade kommissionen i november 2007 fram ett förslag till en sådan ändring av direktivet om integritet och elektronisk kommunikation, vari det bekräftas att RFID-tillämpningar ⁽¹⁾ omfattas av direktivet, men utan att föreslå en utvidgning av direktivets räckvidd till att omfatta privata nätverk,

— göra en bedömning av behovet av ytterligare lagstiftningsåtgärder för att skydda personlig integritet och personuppgifter.

65. Man kan förvänta sig att kommissionen i enlighet med denna politik inte avser att föreslå en ny särskild lagstiftning för skydd av personlig integritet och personuppgifter inom området RFID-teknik, åtminstone inte på kort sikt.

Ramar för lagstiftaren

66. I sitt yttrande om meddelandet om dataskyddsdirektivet angav Europeiska datatillsynsmannen lagstiftningsåtgärder rörande hanteringen av personuppgifter, vilka kan sammanfattas på följande sätt:

— För det första bör grundprincipen för skydd av personuppgifter behållas: "Det behövs inga nya principer, men det finns ett klart behov av andra administrativa lösningar som dels är effektiva och anpassade till nätverkssamhället och dessutom leder till minskade administrativa kostnader" ⁽²⁾.

— För det andra bör lagstiftningsförslag endast läggas fram om det i tillräcklig utsträckning påvisats att det är nödvändigt och proportionellt. Av detta skäl bör den allmänna rättsliga ramen för skydd av personuppgifter inte ändras på kort sikt.

— För det tredje kan utvecklingen i samhället leda till särskilda rättsliga ramar för att anpassa principerna i dataskyddsdirektivet till frågor som väcks av en särskild teknik, som RFID-tekniken. Det står klart att kraven på

nödvändighet och proportionalitet även i detta sammanhang måste vara uppfyllda.

67. Som nästa steg är det lämpligt att närmare ange de förväntningar som lagstiftaren möter på RFID-området:

— Lagstiftningen måste vara flexibel och lämna utrymme för innovationer och teknisk utveckling. Detta bör leda till en lagstiftning som är tillräckligt teknikneutral.

— Som andra steg behöver lagstiftaren erbjuda rättssäkerhet. Detta bör leda till en lagstiftning som är tillräckligt specifik. Intressenter måste exakt veta hur deras agerande är reglerat.

— För det tredje måste lagstiftningen på ett effektivt sätt skydda alla berättigade intressen som står på spel. Detta kräver under alla förhållanden upprätthållande av lagstiftningen och klart fastställda ansvarsförhållanden: vilken part har ansvaret för vilket agerande ⁽³⁾? Dessa krav är ännu mer framträdande när det gäller skydd av personlig integritet och personuppgifter, människans grundläggande rättigheter enligt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och Europeiska unionens stadga om de grundläggande rättigheterna.

Europeiska datatillsynsmannens ståndpunkt

68. Det står helt klart för Europeiska datatillsynsmannen att all teknisk utveckling inte bör leda till åtgärder från de europeiska lagstiftarnas sida. Teknisk utveckling kan gå fort, medan antagande och ikraftträdande av lagstiftning tar tid och bör göra det. Lagstiftning bör vara resultatet av en avvägning mellan samtliga intressen som står på spel. När instrumentet direktiv väljs, behövs ännu mer tid, eftersom direktiv måste genomföras till fullo i medlemsstaternas rättssystem.

69. RFID-tekniken är emellertid inte bara ännu en teknisk utveckling, vilket har framhållits i flera delar i detta yttrande. Meddelandet hänvisar till RFID-tekniken som ingångsporten till en ny utvecklingsfas för informations-samhället, vilket ofta kallas *sakernas internet*, och RFID-etiketter kommer att utgöra huvudelement i den intelligenta miljön. Dessa miljöer är också ett viktiga steg i utvecklingen av vad som ofta kallas *övervakningssamhället* ⁽⁴⁾. Mot denna bakgrund kan det vara berättigat att vidta lagstiftningsåtgärder på detta område. RFID-tekniken kan leda till en kvalitativ förändring.

⁽³⁾ I terminologin som avser skydd av personuppgifter innebär detta en identifiering av *registeransvarig*.

⁽⁴⁾ Detta budskap upprepas i ett uttalande från de europeiska dataskyddsmyndigheterna antaget i London den 2 november 2006, vilket finns tillgängligt på webbplatsen: <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51>

⁽¹⁾ Se föreslagen ny artikel 3 i direktiv 2002/58/EG.

⁽²⁾ Punkt 24 i yttrandet om meddelandet om dataskyddsdirektivet.

70. I detta perspektiv rekommenderar Europeiska datatillsynsmannen att man överväger antagandet av (ett förslag till) gemenskapslagstiftning som reglerar huvudfrågorna när det gäller användningen av RFID-tekniken inom berörda sektorer, om en korrekt tillämpning av den gällande rättsliga ramen inte leder till något resultat. Efter dess ikraftträdande måste en sådan lagstiftningsåtgärd betraktas som *lex specialis* i förhållande till den allmänna ramen för skyddet av personuppgifter.

71. Antagandet av ett sådant rättsligt instrument skulle ge följande fördelar:

- Instrumentet skulle kunna fastställa de väsentliga parametrarna för de självreglerande mekanismerna.
- Möjligheten att ett rättsligt instrument kommer att antas kan tänkas visa sig vara en effektiv sporre för intressenterna att inrätta självreglerande mekanismer som ger ett korrekt skydd.

72. För att göra det mer praktiskt skulle kommissionen kunna anmodas att utarbeta dokument för samråd om för- och nackdelarna med en särskild lagstiftning och om huvuddelarna i en sådan lagstiftning. Intressenterna kan naturligtvis ombes att bidra till detta samråd. Artikel 29-arbetsgruppen kan också delta.

Möjliga sätt

73. Lagstiftarens intervention skulle kunna ombesörja en skräddarsydd rättslig ram, som består av en blandning av regleringsinstrument som specificerar och kompletterar den nu gällande rättsliga ramen. Denna skräddarsydda rättsliga ram bör vara baserad på kända principer för skydd av personuppgifter och bör inriktas på fördelning av ansvar och på effektivitet hos kontrollmekanismerna.

74. Ett särskilt skäl för att en sådan skräddarsydd lagstiftning kan behövas är att inte alla RFID-tillämpningar medför en hantering av personuppgifter. Om RFID-tillämpningar med andra ord inte innebär hantering av personuppgifter, är de parter som är involverade i framställning och försäljning av aktiva RFID-produkter inte juridiskt bundna att vidta några tekniska åtgärder för att förhindra smyglysning eller uppsättning av läsare utan att informera enskilda individer om detta. Som påvisats finns det ändå risk för den personliga integriteten när det gäller sådana RFID-tillämpningar, genom möjligheten att övervaka enskilda individer, och det krävs därför samma typ av skyddsåtgärder för den personliga integriteten. Det kan vara fallet vid etikettmärkning av konsumentprodukter innan de kommer till försäljningsstället. Sammanfattningsvis kan RFID-tillämpningar som inte hanterar personuppgifter fortfarande utgöra ett hot mot den personliga integriteten genom att de möjliggör en dold övervakning och användning av informationen för oacceptabla syften.

75. Europeiska datatillsynsmannen anser att denna olyckliga utgång bör undvikas. Eftersom nu gällande lagstiftning delvis, åtminstone när det gäller RFID-tillämpningar som inte hanterar personuppgifter, misslyckas med att möta detta hot mot den personliga integriteten och med tanke på tillkortakommandena när det gäller lösningar med icke-bindande regler, tycks det vara nödvändigt att använda tvingande rättsliga åtgärder för att säkerställa ett tillfredställande resultat.

76. Sådana åtgärder bör under alla förhållanden

- fastställa principen om frivilligt deltagande vid försäljningsstället som en klar och obestridlig rättslig skyldighet, även för RFID-tillämpningar som faller utanför räckvidden för dataskyddsdirektivet ⁽¹⁾,
- säkerställa en obligatorisk utveckling av RFID-tillämpningar med lämplig teknisk konstruktion, såsom mekanismer för att skydda den personliga integriteten (*privacy by design*).

VII. FÖRVALTNING

77. Även om den inneboende gränsöverskridande dimensionen hos RFID-systemen i meddelandet endast behandlas inom den inre marknaden, anser Europeiska datatillsynsmannen att denna dimension måste hanteras på en vidare internationell nivå. RFID-systemen är redan *gränsöverskridande* i butiken, eftersom etiketten kanske inte upphör att vara verksam på försäljningsstället. När det gäller det övergripande RFID-systemet, blir denna teknik *gränsöverskridande* när överföring av personuppgifter till tredjeland kan ske om tillverkaren av den etiketterade artikeln, som omfattas av ett RFID-system, är baserad utanför Europeiska unionen ⁽²⁾.

78. Ur ett framtidsperspektiv utgör också förvaltningen av RFID-systemens referensdatabaser en viktig dimension för en korrekt efterlevnad av den europeiska rättsliga ramen för skydd av personuppgifter. Europeiska datatillsynsmannen uppmanar enträget till att man finner en lösning, eftersom en ytterligare erodering av den rättsliga ramen inte kan accepteras.

79. Europeiska datatillsynsmannen förutser att förvaltningen av RFID-tekniken kommer att utgöra en betydande utmaning och kräva avsevärda investeringar. Man måste komma fram till vad som är rätt forum för förhandlingar och en lämplig infrastruktur för styrning för att säkerställa att rätten till skydd av personuppgifter respekteras på ett korrekt sätt i dessa internationella miljöer.

⁽¹⁾ I avsnitt IV hävdas att principen om frivilligt deltagande vid försäljningsstället redan finns som en rättslig skyldighet enligt dataskyddsdirektivet.

⁽²⁾ De skyldigheter som är förbundna med överföring av personuppgifter behandlas i artiklarna 25 och 26 i dataskyddsdirektivet.

80. Med tanke på detta uppmanar Europeiska datatillsynsmannen kommissionen att lägga fram sina synpunkter om förvaltning, möjligen i samråd med RFID-intressenterna.

VIII. SLUTSATSER

81. Datatillsynsmannen välkomnar kommissionens meddelande om RFID-tekniken, eftersom det tar upp huvudfrågorna i samband med spridningen av RFID-teknik utan att försumma de avgörande frågorna som hänför sig till skydd av personlig integritet och personuppgifter. Datatillsynsmannen instämmer i synpunkten att RFID-systemen kan komma att spela en avgörande roll i utvecklingen av informationssamhället, något som man vanligen hänvisar till som "sakernas internet".

Klargörande av konsekvenserna

82. Den utbredda användningen av RFID-tekniken är något grundläggande nytt och kan få avgörande inverkan på vårt samhälle och på skyddet för grundläggande rättigheter i vårt samhälle, så som rätt till skydd av personlig integritet och personuppgifter. RFID-tekniken kan leda till en kvalitativ förändring.

83. Fem grundläggande frågor rörande personlig integritet och säkerhet kan urskiljas:

- Identifiering av den person som uppgifterna gäller.
- Identifiering av den/de registeransvariga.
- Den minskade innebörden av den traditionella skillnaden mellan den privata och den offentliga sfären.
- Konsekvenserna av RFID-etiketternas storlek och fysiska egenskaper.
- Avsaknaden av insyn och öppenhet i processen.

Närmare angivande av konsekvenserna

84. Den allmänna rättsliga ramen för skydd av personuppgifter i enlighet med direktiv 95/46/EG gäller RFID i den utsträckning som de uppgifter som hanteras av RFID-systemen omfattas av definitionen av personuppgifter.

85. När det gäller direktivet om integritet och elektronisk kommunikation: Kommissionens förslag av den 13 november 2007 om ändring av detta direktiv innehåller en bestämmelse med syfte att fastställa att direktivet förvisso gäller vissa RFID-tillämpningar. Men vissa andra RFID-tillämpningar omfattas eventuellt inte på grund av att tillämpningen av direktivet är begränsad till behandling av personuppgifter i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät.

86. Skyddet av personuppgifter kan kompletteras med en rad självreglerande instrument. Det är lämpligt att lämna utrymme för sådan självreglering under förutsättning att

— den ger konkret och praktisk vägledning om specifika typer av RFID-tillämpningar,

— den åtgärdar de specifika frågor som rör skyddet av personuppgifter och de problem som uppstår i samband med generella RFID-tillämpningar,

— den bidrar till en enhetlig och harmoniserad tillämpning av dataskyddsdirektivet inom hela EU,

— den tillämpas av samtliga berörda intressenter.

87. Europeiska datatillsynsmannen rekommenderar kommissionen att i nära samarbete med RFID-expertgruppen ta fram ett eller flera dokument med en klar vägledning om på vilket sätt den nuvarande rättsliga ramen ska tillämpas på RFID-miljön.

88. Vägledningen med principerna för användningen av RFID-tekniken bör vara tillräckligt fokuserad och införa ett synsätt som är specifikt för detta område. Den bör föreslå praktiska och effektiva metoder för utvecklingen av metoder och normer som kan bidra till att RFID-systemen uppfyller bestämmelserna i den rättsliga ramen för skydd av personuppgifter och kommer att innebära användandet av en teknik med inbyggda skyddsmekanismer för den personliga integriteten (privacy by design).

89. Europeiska datatillsynsmannen välkomnar att kommissionen i meddelandet tillstyrker idén om att specificera och införa kriterier för utformningen i ett tidigt skede.

90. Även om datatillsynsmannen anser att principen om frivilligt deltagande vid försäljningsstället är en lagstadgad skyldighet som i de flesta fall redan gäller i enlighet med dataskyddsdirektivet, bör denna skyldighet specificeras i de självreglerande instrumenten.

Behöver särskilda åtgärder vidtas?

91. För att användningen av begreppet inbyggda skyddsmekanismer för den personliga integriteten (privacy by design) ska bli obligatoriskt rekommenderar Europeiska datatillsynsmannen att kommissionen använder sig av mekanismen i artikel 3.3 c i direktiv 1999/5/EG i samråd med expertgruppen för RFID.

92. Europeiska datatillsynsmannen rekommenderar att man överväger antagandet av (ett förslag till) gemenskapslagstiftning som reglerar huvudfrågorna för användningen av RFID-tekniken inom berörda sektorer om en korrekt tillämpning av den gällande rättsliga ramen inte leder till något resultat. Efter dess ikraftträdande måste en sådan lagstiftning betraktas som *lex specialis* i förhållande till den allmänna ramen för skydd av personuppgifter. Lagstiftningsåtgärderna bör också ta upp skydd för personlig integritet och personuppgifter när det gäller vissa RFID-tillämpningar, som etikettering av artiklar före försäljningsstället, vilket inte nödvändigtvis medför bearbetning av personuppgifter.

93. Kommissionen bör utarbeta ett dokument för samråd om fördelar och nackdelar med särskild lagstiftning och de huvudsakliga beståndsdelarna i en sådan lagstiftning.
94. Lagstiftarens intervention skulle kunna ombesörja en skräddarsydd rättslig ram, som består av en blandning av regleringsinstrument som specificerar och kompletterar den nu gällande rättsliga ramen. Åtgärderna bör under alla förhållanden
- fastställa principen om frivilligt deltagande vid försäljningsstället som en klar och obestridlig rättslig skyldighet, även för RFID-tillämpningar som faller utanför räckvidden för dataskyddsdirektivet ⁽¹⁾,
 - säkerställa obligatorisk utveckling av RFID-tillämpningar med lämplig teknisk konstruktion, såsom mekanismer

för att skydda den personliga integriteten (privacy by design).

Frågan om förvaltning

95. Europeiska datatillsynsmannen uppmanar kommissionen att lägga fram sina synpunkter om förvaltning, möjligen i samråd med RFID-intressenterna.

Bryssel den 20 december 2007.

Peter HUSTINX
Europeiska datatillsynsmannen

⁽¹⁾ I avsnitt IV hävdas att principen om frivilligt deltagande vid försäljningsstället redan finns som en rättslig skyldighet enligt dataskyddsdirektivet.