I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om att främja förtroendet för informationssamhället genom stärkt data- och integritetsskydd

(2010/C 280/01)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 och 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 ([1]),

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 ([2]),

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 ([3]), särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. Informations- och kommunikationsteknik (IKT) öppnar upp för enorma möjligheter inom praktiskt taget alla delar av våra liv – hur vi arbetar, tillbringar vår fritid, umgås med varandra och utbildar oss. IKT är av avgörande betydelse för dagens informationsekonomi och för samhället i stort.

2. Europeiska unionen är en global kraft på området avancerad informations- och kommunikationsteknik, en ställning den är fast besluten att behålla. För att möta denna utmaning förväntas Europeiska kommissionen inom kort att anta en ny digital dagordning för Europa, något som kommissionsledamot Neelie Kroes har bekräftat som sin prioritet ([4]).

3. Datatillsynsmannen erkänner de fördelar som IKT för med sig och håller med om att EU bör göra sitt yttersta för att främja utvecklingen av IKT och se till att denna teknik införs på bred front. Datatillsynsmannen delar vidare fullt ut kommissionsledamöterna Kroes och Redings åsikt om att individerna bör sättas i centrum i denna nya miljö ([5]). Enskilda personer bör kunna lita på informations- och kommunikationsteknikens förmåga att skydda deras uppgifter och kontrollera hur de används, samt att deras rättigheter till integritets- och dataskydd kommer att respekteras i den digitala världen. Att dessa rättigheter respekteras är avgörande för att skapa ett förtroende hos konsumenterna och ett sådant förtroende är i sin tur avgörande för att medborgarna ska acceptera nya tjänster ([6]).

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 201, 31.7.2002, s. 37.
([3]) EGT L 8, 12.1.2001, s. 1.

([4]) Svar på Europaparlamentets skriftliga frågor till kommissionsledamot Neelie Kroes i samband med Europaparlamentets utfrågningar inför kommissionsledamotens utnämning.
([5]) Svar på Europaparlamentets skriftliga frågor till kommissionsledamot Neelie Kroes i samband med Europaparlamentets utfrågningar inför kommissionsledamotens utnämning. Kommissionsledamot Viviane Redings tal på ämnet ”A European Digital Agenda for the New Digital Consumer” vid BEUC:s ”Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives” i Bryssel den 12 november 2009.
([6]) Se t.ex. RISEPTIS rapport *Trust in the Information Society*, en rapport från den rådgivande nämnden, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society) på http://www.think-trust.eu/general/news-events/riseptis-report.html. Se även J. B Horrigan, ”Broadband Adoption and Use in America”, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. EU har en stark rättslig ram för data- och integritetsskyddet, vars principer tillämpas fullt ut även i den digitala tidsåldern. Därmed inte sagt att det går att slå sig till ro. I flera fall ger IKT upphov till nya frågeställningar som inte omfattas av den befintliga ramen, vilket gör det nödvändigt att vidta åtgärder för att se till att enskilda personers rättigheter, enligt vad som fastställs i EU:s lagstiftning, också framöver omfattas av ett effektivt skydd även i denna nya miljö.

5. I det här yttrandet diskuteras de åtgärder som Europeiska unionen skulle kunna främja eller vidta för att säkerställa enskilda personers data- och integritetsskydd i en fortsatt teknikdriven globaliserad värld. Yttrandet tar upp lagstiftande och icke lagstiftande instrument.

6. Efter att först ha gett en översikt över IKT som en ny teknikutveckling som skapar möjligheter men även ger upphov till risker, går yttrandet vidare till att diskutera behovet av att data- och integritetsskyddet finns med redan när ny informations- och kommunikationsteknik utformas (nedan kallat *principen om* ”privacy by design”). För att säkerställa att denna princip iakttas diskuterar yttrandet behovet att införliva principen om ”privacy by design” i den rättsliga ramen för dataskydd på minst två olika sätt. För det första genom att införliva den som en allmän, bindande princip och, för det andra, genom att införliva den inom särskilda IKT-områden där de särskilda risker för data- och integritetsskyddet som uppstår kan reduceras genom lämplig teknisk arkitektur och design. Det rör sig om följande områden: RFID (Radio Frequency Identification), mötesplatser på nätet och tillämpningar via webbläsare. Slutligen lägger yttrandet fram förslag på andra verktyg och principer som syftar till att skydda enskilda personers integritets- och dataskydd inom IKT-sektorn.

7. Genom att ta upp dessa frågor behandlar datatillsynsmannen i detta yttrande några av de åsikter som artikel 29-arbetsgruppen lagt fram i sitt bidrag till det offentliga samrådet om det framtida integritetsskyddet ([1]). Yttrandet bygger även på tidigare yttranden från datatillsynsmannen, t.ex. yttrandet av den 25 juli 2007 om genomförandet av dataskyddsdirektivet, yttrandet av den 20 december 2007 om RFID och de två yttrandena om direktivet om integritet och elektronisk kommunikation ([2]).

II. IKT ERBJUDER NYA MÖJLIGHETER MEN SKAPAR OCKSÅ NYA RISKER

8. IKT har jämförts med andra banbrytande uppfinningar, t.ex. elektriciteten. Även om det kanske är för tidigt att bedöma den konkreta effekten på vår historia, finns det ett klart samband mellan IKT och ekonomisk tillväxt i utvecklade länder. IKT har skapat sysselsättning, ekonomiska fördelar och bidragit till länders allmänna välfärd. Effekterna av IKT går utöver de rent ekonomiska, eftersom den har spelat en viktig roll för att främja innovation och kreativitet.

9. IKT har dessutom förändrat det sätt på vilket vi arbetar, umgås och interagerar med varandra. Människor använder sig till exempel i allt högre grad av IKT i sina ekonomiska och sociala liv. Enskilda personer kan i allt större utsträckning använda en lång rad nya IKT-tillämpningar, t.ex. e-hälsovård, e-transport, e-förvaltning samt innovativa interaktiva system för underhållning och inlärning.

10. Mot bakgrund av dessa fördelar har samtliga av de europeiska institutionerna förbundit sig att stödja IKT som ett nödvändigt verktyg för att förbättra den europeiska industrins konkurrenskraft och för att skynda på Europas ekonomiska återhämtning. I augusti 2009 antog kommissionen sitt meddelande *Europeisk rapport om digital konkurrenskraft* ([3]) och inledde ett offentligt samråd om lämpliga framtida strategier för att främja IKT. Den 7 december 2009 lade rådet fram ett bidrag till detta samråd genom sina slutsatser: Post i2010-strategin – Mot ett öppet, grönt och konkurrenskraftigt kunskapssamhälle ([4]). Europaparlamentet har nyligen

([1]) Artikel 29-arbetsgruppens yttrande 168 om ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, antaget den 1 december 2009.

([2]) Yttrande av den 25 juli 2007 om meddelandet från kommissionen till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, EUT C 255, 27.10.2007, s. 1. Yttrande av den 20 december 2007 kommissionens meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om *Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi*, (KOM(2007) 96), EUT C 101, 23.4.2008, s. 1. Yttrande av den 10 april 2008 om förslaget till Europaparlamentets och rådets direktiv om ändring av bland annat direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EUT C 181, 18.7.2008, s. 1. Andra yttrandet av den 9 januari 2009 om översynen av direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

([3]) Europeisk rapport om digital konkurrenskraft – De största landvinningarna för strategin i2010 under 2005–2009, (SEC (2009) 1060).

([4]) Rådets slutsatser: Post i2010-strategin – Mot ett öppet, grönt och konkurrenskraftigt kunskapssamhälle, (17107/09), antagna den 18.12.2009.

antagit ett betänkande som syftar till att ge kommissionen vägledning för att definiera en digital agenda ([1]).

11. Vid sidan av de möjligheter och fördelar som utvecklingen av IKT för med sig skapas även nya risker, särskilt med avseende på den personliga integriteten och skyddet av enskilda personers personuppgifter. IKT leder ofta till att den mängd information som samlas in, sorteras, filtreras, överförs eller på annat sätt behålls sprids (ofta på sätt som enskilda personer inte är medvetna om), vilket innebär att de risker som är förknippade med detta ökar.

12. Ett exempel på detta är de RFID-taggar som nu ersätter streckkoder på (vissa) konsumentprodukter. Genom att förbättra informationsflödet i försörjningskedjan (och därigenom kunna minska behovet av "säkerhets"-lager, tillhandahålla mer korrekta prognoser etc.) förväntas det nya systemet gynna både företagen och konsumenterna. Samtidigt ökar detta emellertid på ett oroväckande sätt möjligheten att spåra enskilda personer, av olika skäl och av olika enheter, genom taggade personliga ägodelar.

13. Ett annat exempel är "cloud computing" (s.k. datormoln), vilket i stort sett går ut på att tillhandahålla webbapplikationer till privatpersoner och företag över Internet. Det kan röra sig om allt från fotobibliotek, kalendrar, webbmail och kunddatabaser till mer komplexa företagstjänster. Fördelarna för både företag och privatpersoner är tydliga: kostnadsreducering (inkrementella kostnader), platsoberoende åtkomlighet (enkelt tillgång till information var som helst i världen), automation (inget behov av särskilda IT-resurser eller av uppdateringar av programvara) etc. Samtidigt föreligger mycket konkreta risker för säkerhetsglapp och hacking. Det finns också en oro för att man ska förlora tillgången till och kontrollen över sina egna data.

14. Fördelar och risker har visat sig samexistera inom andra områden där man använder sig av IKT-tillämpningar. Ta till exempel e-hälsovård, som kan förbättra effektiviteten, sänka kostnaderna, öka tillgängligheten och allmänt förbättra kvaliteten på hälsovårdstjänster. E-hälsovård ger emellertid också upphov till frågan om legitimiteten hos sekundär användning av hälsouppgifter, vilket kräver en ingående analys av syftena med eventuell sekundär användning ([2]). Eftersom elektroniska patientjournalen nu används i allt större utsträckning har systemen själva drabbats av skandaler där man i flera fall avslöjat hackers som olagligt tagit sig in i elektroniska patientjournaler.

15. För att sammanfatta är det sannolikt att det alltid kommer att finnas en viss kvarstående risk, även efter korrekta bedömningar och tillämpning av nödvändiga åtgärder. Samtidigt som det skulle vara orealistiskt att förvänta sig en helt riskfri situation kan och måste emellertid åtgärder vidtas för att minska sådana risker till lämpliga nivåer (se nedan).

III. "PRIVACY BY DESIGN" SOM ETT AVGÖRANDE VERKTYG FÖR ATT SKAPA FÖRTROENDE FÖR IKT HOS ENSKILDA PERSONER

16. Frukterna av de potentiella fördelarna med IKT kan endast skördas om denna teknik kan skapa ett förtroende, dvs. om den kan få användarna att vilja utnyttja IKT till följd av denna tekniks egenskaper och fördelar. Ett sådant förtroende kommer endast att kunna vinnas om informations- och kommunikationstekniken är tillförlitlig och säker, om enskilda personer har kontroll över den och om skyddet av individernas personuppgifter och integritet garanteras.

17. Sådana omfattande risker och misslyckanden som de som beskrivits ovan kommer, särskilt om de inbegriper missbruk av personuppgifter eller överträdelser av personuppgiftsbestämmelser som exponerar enskilda personers privatliv, sannolikt att äventyra användarnas förtroende för informationssamhället. Detta skulle allvarligt kunna skada utvecklingen av och fördelarna med IKT.

18. Att eliminera dessa risker med avseende på data- och integritetsskyddet genom att undanröja, exkludera eller vägra att använda eller främja IKT är dock inte ett alternativ. Det skulle varken vara genomförbart eller realistiskt och hindra enskilda personer från att dra nytta av fördelarna med IKT samt allvarligt begränsa de övergripande fördelarna med denna teknik.

19. Europeiska datatillsynsmannen anser att en mer positiv lösning är att utforma och utveckla IKT på ett sätt som respekterar data- och integritetsskyddet. Det är därför av allra största vikt att detta skydd finns med under teknikens hela livscykel, från utformningsstadiet fram till dess att den slutligen tas i bruk och så småningom skrotas. Detta kallas normalt "privacy by design" och diskuteras vidare nedan.

20. "Privacy by design" kan inbegripa flera olika åtgärder, beroende på det särskilda fallet eller tillämpningen. I vissa fall kan det till exempel krävas att personuppgifter tas bort/reduceras eller att onödig och/eller oönskad behandling av personuppgifter förhindras. I andra fall kan "privacy by design" innebära att man tillhandahåller verktyg som ökar användarnas kontroll över sina personuppgifter.

([1]) Betänkande om fastställandet av en ny digital agenda för Europa: från i2010 till digital.eu (2009/2225 (INI)), antaget den 18.3.2010.

([2]) Försäljning eller användning av hälsouppgifter som samlats in i syfte att behandla en patient får exempelvis inte användas för att välja platser för satellitkliniker, att etablera ambulerande kirurgi, och på andra sätt planera framtida aktiviteter med finansiella konsekvenser skulle kräva noggrann granskning.

Sådana åtgärder skulle kunna övervägas vid definitionen av standarder och/eller bästa metoder. De skulle också kunna införlivas i informations- och kommunikationssystemens arkitektur, eller i de strukturella organisationerna hos de enheter som behandlar personuppgifter.

III.1 **Tillämpning av principen om ”privacy by design” inom olika IKT-områden och effekten av detta**

21. Det finns ett behov av principen om ”privacy by design” inom en rad olika IKT-områden. Inom till exempel hälso- och sjukvårdssektorn används i allt högre grad IKT-infrastrukturer som ofta inbegriper en centraliserad lagring av patientjournaler. En tillämpning av principen om ”privacy by design” inom hälso- och sjukvårdssektorn skulle kräva en bedömning av olika åtgärders lämplighet, t.ex. möjligheten att minimera data som lagras centralt eller en begränsning av sådana data till ett index, användning av krypteringsverktyg, att endast ge de som absolut behöver det tillträdesrätt, en anonymisering av data när de inte längre behövs etc.

22. Inom transportsektorn förses transportsystem allt oftare automatiskt med avancerade IKT-tillämpningar som interagerar med fordonet och dess miljö för olika syften och funktioner. Bilar utrustas till exempel i allt högre grad med nya IKT-funktioner (GPS, GSM, nätverk av sensorer etc.) som inte bara visar var fordonet befinner sig utan även dess tekniska förhållanden i realtid. Denna information skulle kunna användas för att exempelvis ersätta befintliga vägskattesystem med vägavgifter som är kopplade till utnyttjandet av olika vägar. Att tillämpa principen om ”privacy by design” vid utformningen av arkitekturen för sådana system skulle innebära att så få personuppgifter som möjligt behandlades och skickades vidare ([1]). I enlighet med denna princip skulle en decentraliserad eller delvis decentraliserad systemarkitektur som begränsar spridning av lokaliseringsuppgifter till en central punkt vara att föredra framför en centraliserad systemarkitektur.

23. Av ovan nämnda exempel framgår att när informations- och kommunikationsteknik bygger på principen om ”privacy by design” är det möjligt att kraftigt minska riskerna med avseende på data- och integritetsskyddet.

III.2 **Otillräckligt utnyttjande av IKT som tillämpar ”privacy by design”**

24. En viktig fråga är huruvida ekonomiska aktörer, tillverkare/tillhandahållare av IKT och registeransvariga har ett intresse av att marknadsföra och genomföra principen om ”privacy by design” inom IKT. I detta sammanhang är det också viktigt att bedöma användarnas behov av ”privacy by design”.

25. Under 2007 utfärdade kommissionen ett meddelande i vilket den uppmanade företag att använda sin förmåga till innovation för att utveckla och genomföra integrationsfrämjande teknik för att förbättra data- och integritetsskyddet redan från början av utvecklingscykeln ([2]).

26. Hittills har emellertid tillgängliga uppgifter visat att varken IKT-tillverkare eller registeransvariga (varken inom den privata eller offentliga sektorn) konsekvent har lyckats genomföra eller marknadsföra principen om ”privacy by design”. Man har lagt fram olika skäl till detta, bland annat bristen på ekonomiska incitament och institutionellt stöd, otillräcklig efterfrågan etc ([3]).

27. Samtidigt har användarna ställt relativt låga krav på ”privacy by design”. Användare av IKT-produkter och IKT-tjänster kanske med rätta tar för givet att deras personliga integritet och personuppgifter är skyddade fastän det i flera fall inte är på det viset. I vissa fall har användarna helt enkelt inte möjlighet att vidta de säkerhetsåtgärder som är nödvändiga för att skydda sina egna eller andras personuppgifter. I flera fall beror detta på att de inte helt eller ens delvis känner till riskerna. Ungdomar bryr sig exempelvis i allmänhet inte om de risker för den personliga integriteten som är förknippade med att lägga ut personuppgifter på nätet och struntar ofta i sekretessinställningarna. Andra användare kanske är medvetna om riskerna men har inte den tekniska kunskap som krävs för att kunna tillämpa den säkerhetsteknik som finns tillgänglig, t.ex. teknik som skyddar deras internetanslutning eller som används för att ändra inställningarna i webbläsaren i syfte att minimera användarprofilering som grundas på övervakning av deras internetsurfande.

28. Riskerna i fråga om data- och integritetsskyddet är emellertid ofta mycket påtagliga. Om detta skydd inte beaktas från första början är det ofta för sent och allt för ekonomiskt betungande att fixa systemen, och ofta för sent att

([1]) Se yttrande från Europeiska datatillsynsmannen av den 22 juli 2009 om kommissionens meddelande om en handlingsplan för införande av intelligenta transportssystem i EU och det åtföljande förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt, tillgänglig på: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Meddelande från kommissionen till Europaparlamentet och rådet om främjande av dataskydd genom integritetsfrämjande teknik, KOM(2007) 228 slutlig, 2.5.2007.

([3]) ”Study on the economic benefits of privacy enhancing technologies (PETS)”, jls/2008/D4/036.

reparera den skada som redan skett. Det ökade antalet dataintrång på senare tid visar tydligt på detta problem och understryker behovet av ”privacy by design”.

29. Av ovan framgår tydligt att tillverkare och tillhandahållare av informations- och kommunikationsteknik som syftar till att behandla personuppgifter bör, tillsammans med registeransvariga, ha ett ansvar att utforma denna teknik med inbyggda skyddsåtgärder för data- och integritetsskyddet. I flera fall skulle detta innebära att denna teknik redan från början utformas med förvalda inställningar för sekretess.

30. Mot denna bakgrund måste vi överväga vilka åtgärder beslutsfattarna bör vidta för att främja ”privacy by design” i utvecklingen av IKT. En första fråga är huruvida den befintliga rättsliga ramen för dataskyddet innehåller tillräckliga bestämmelser för att säkerställa att både registeransvariga och tillverkare/utvecklare genomför principen om ”privacy by design”. En andra fråga man måste ställa sig är vad som bör göras inom ramen för den digitala dagordningen för Europa för att se till att IKT-sektorn skapar förtroende hos konsumenterna.

IV. ATT INFÖRLIVA PRINCIPEN OM ”PRIVACY BY DESIGN” I EU:s LAGSTIFTNING OCH POLITIK

IV.1 Den befintliga rättsliga ramen för data- och integritetsskyddet

31. EU har ett starkt ramverk för data- och integritetsskyddet som fastställs i direktiv 95/46/EG [1], direktiv 2002/58/EG [2] samt i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna [3] och EG-domstolen.

32. Dataskyddsdirektivet är tillämpligt på ”åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter” (insamling, lagring, utlämnande etc.). I direktivet föreskrivs att de som behandlar personuppgifter (”registeransvariga”) måste iaktta vissa principer och skyldigheter. Vidare fastställs enskilda personers rättigheter, t.ex. rätten att få tillgång till sina egna personuppgifter. Direktivet om integritet och elektronisk kommunikation behandlar särskilt integritetsskyddet inom sektorn för elektronisk kommunikation [4].

33. Det befintliga dataskyddsdirektivet innehåller inte något uttryckligt krav på ”privacy by design”. Däremot innehåller det bestämmelser som indirekt, i olika situationer, mycket väl skulle kunna kräva genomförandet av principen om ”privacy by design”. Enligt artikel 17 krävs bland annat att registeransvariga ska genomföra lämpliga tekniska och organisatoriska åtgärder för att förhindra otillåten behandling av uppgifter [5]. ”Privacy by design” täcks följaktligen på ett mycket allmänt sätt. Dessutom riktar sig bestämmelserna i direktivet främst till registeransvariga och det sätt på vilket de behandlar personuppgifter. Bestämmelserna kräver inte uttryckligen att data- och integritetsskyddet måste byggas in i informations- och kommunikationstekniken – detta skulle kräva att de även riktar sig till utvecklare och tillverkare av IKT, inbegripet de verksamheter som utförs under standardiseringsfasen.

34. Direktivet om integritet och elektronisk kommunikation är mer utförligt. I artikel 14.3 föreskrivs följande: ”När så krävs får åtgärder vidtas för att säkerställa att terminalutrustning är konstruerad så att den är förenlig med användarnas rätt till skydd och kontroll av sina personuppgifter i enlighet med direktiv 1999/5/EG och rådets beslut 87/95/EEG av den 22 december 1986 om standardisering inom området informationsteknologi och telekommunikation.” Denna bestämmelse har emellertid aldrig använts [6].

35. Även om de ovan nämnda bestämmelserna i de två direktiven bidrar till att *främja* ”privacy by design”, har de i praktiken inte varit tillräckliga för att *säkerställa* att skyddsmekanismer för den personliga integriteten byggs in i IKT.

36. Lagen kräver alltså inte på ett tillräckligt klart sätt att IKT utformas i enlighet med principen om ”privacy by design”. Dessutom har dataskyddsmyndigheter inte tillräckliga befogenheter för att säkerställa ett införlivande av principen om ”privacy by design”. Detta leder till ineffektivitet. Dataskyddsmyndigheter skulle exempelvis kunna införa påföljder i fall där förfrågningar om tillgång från enskilda personer inte besvaras och har befogenhet att kräva att

(1) Europaparlamentets och rådets direktiv 95/46/EG (dataskyddsdirektivet).

(2) Europaparlamentets och rådets direktiv 2002/58/EG (direktivet om e-integritet).

(3) Tolkning av de viktigaste delarna och villkoren i artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, antagen i Rom den 4 november 1950, i deras olika tillämpningar.

(4) Lissabonfördraget har förstärkt detta skydd genom att erkänna respekten för privatlivet och skyddet av personuppgifter som separata grundläggande rättigheter i artiklarna 7 och 8 i EU:s stadga om de grundläggande rättigheterna som blev bindande när Lissabonfördraget trädde i kraft.

(5) Artikel 17 lyder enligt följande: ”Medlemsstaterna skall föreskriva att den registeransvarige skall genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.” Detta kompletteras med skäl 46: ”Skyddet för de registrerades fri- och rättigheter förutsätter så vitt avser behandling av personuppgifter att lämpliga tekniska och organisatoriska åtgärder vidtas både när systemet för behandlingen utformas och när själva behandlingen sker, särskilt för att garantera säkerheten och för att på så sätt hindra all otillåten behandling.”

(6) Kommissionen har meddelat sin avsikt att uppdatera direktiv 1999/5/EG i slutet av 2010.

vissa åtgärder vidtas för att förhindra otillåten behandling av uppgifter. Det står emellertid inte alltid klart om deras befogenheter sträcker sig så långt som till att kräva att ett system utformas på ett sätt som främjar enskilda personers personuppgiftsskydd ([1]). Av de befintliga rättsliga bestämmelserna framgår till exempel inte om man har rätt att kräva att en informationssystemarkitektur utformas på ett sätt som gör det enklare för företag att besvara förfrågningar om tillgång från enskilda personer så att sådana förfrågningar kan hanteras automatiskt och snabbare. Dessutom kan senare försök att ändra tekniken när den väl har utvecklats eller satts i bruk leda till ett lapptäcke av lösningar som inte fungerar fullt ut, och dessutom vara ekonomiskt betungande.

37. Enligt Europeiska datatillsynsmannens åsikt, som delas av artikel 29-arbetsgruppen ([2]), finns det utrymme i den gällande rättsliga ramen för ett mer uttryckligt godkännande av principen om ”privacy by design”.

IV.2 **Att införliva ”privacy by design” på olika nivåer**

38. Mot bakgrund av ovanstående rekommenderar Europeiska datatillsynsmannen att kommissionen följer fyra handlingslinjer:

a) Att lägga fram ett förslag som inkluderar en allmän bestämmelse om ”privacy by design” i den rättsliga ramen för dataskydd.

b) Att vidareutveckla denna allmänna bestämmelse i särskilda bestämmelser i samband med att förslag till särskilda rättsliga instrument för olika sektorer läggs fram. Dessa särskilda bestämmelser skulle redan nu kunna inkluderas i rättsliga instrument, på grundval av artikel 17 i dataskyddsdirektivet (och annan befintlig lagstiftning).

c) Att inkludera ”privacy by design” som en vägledande princip i den digitala dagordningen för Europa.

d) Att införa ”privacy by design” som en princip i andra EU-initiativ (främst icke lagstiftande).

En allmän bestämmelse om ”privacy by design”

39. Europeiska datatillsynsmannen föreslår att principen om ”privacy by design” uttryckligen och entydigt inkluderas i den befintliga rättsliga ramen för dataskydd. Detta skulle förstärka denna princip, göra den mer uttrycklig och tvinga fram ett effektivt genomförande av den, samtidigt som det ger tillsynsmyndigheterna ökade befogenheter att kräva att den faktiskt tillämpas i praktiken. Detta är framför allt nödvändigt mot bakgrund av det som angivits ovan, inte bara eftersom principen i sig är ett viktigt verktyg för att främja ett förtroende, utan även som ett incitament för berörda aktörer att genomföra ”privacy by design” och stärka de garantier som föreskrivs i den befintliga rättsliga ramen.

40. Detta förslag bygger på artikel 29-arbetsgruppens rekommendation att införa principen om ”privacy by design” som en allmän princip i den rättsliga ramen för dataskydd, däribland dataskyddsdirektivet. Enligt artikel 29-arbetsgruppen bör denna princip vara bindande för teknikutvecklare och tillverkare samt för registeransvariga som ska besluta om förvärv och användning av IKT. De bör åläggas att ta hänsyn till tekniken för dataskydd redan vid planeringsstadiet för informationstekniska förfaranden och system. Tillhandahållare av sådana system eller tjänster samt registeransvariga bör kunna visa att de har vidtagit alla åtgärder som krävs för att iaktta dessa krav.

41. Europeiska datatillsynsmannen välkomnar vidare kommissionsledamot Viviane Redings stöd för principen om ”privacy by design”, som hon gav uttryck för i samband med meddelandet om granskningen av dataskyddsdirektivet ([3]).

42. Vad gäller innehållet i en sådan reglering är det första och viktigaste att en allmän princip om ”privacy by design” är teknikneutral. Principen bör inte ha för avsikt att reglera tekniken och bör alltså inte föreskriva särskilda tekniska lösningar utan i stället att befintliga principer för integritets- och dataskyddet ska integreras i informations- och

([1]) Se den brittiska informationskommissionärens rapport *Privacy by Design*, publicerad i november 2008.

([2]) Se artikel 29-gruppens yttrande om ”The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, antaget den 1 december 2009.

([3]) ” ’Privacy by design’ är en princip som ligger i både medborgarnas och företagens intresse. ’Privacy by design’ kommer att leda till ett bättre skydd för enskilda personer, samt till ett förtroende för och en tillit till nya tjänster och produkter, vilket i sin tur kommer att ha en positiv inverkan på ekonomin. Det finns flera uppmuntrande exempel, men fortfarande återstår mycket arbete.” Huvudtal vid dataskyddsdagen den 28 januari 2010, Europaparlamentet, Bryssel.

kommunikationssystem och lösningar. Detta skulle göra det möjligt för berörda parter, tillverkare, registeransvariga och dataskyddsmyndigheter att i varje enskilt fall tolka innebörden i principen. För det andra skulle ett iakttagande av principen vara obligatoriskt i alla steg, från utformningen av standarder och arkitektur till dess att de genomförs av registeransvariga.

Bestämmelser i särskilda rättsinstrument

43. Befintliga och framtida lagstiftningsinstrument måste integrera principen om ”privacy by design” på grundval av den befintliga rättsliga ramen och, efter antagandet av den ovan föreslagna allmänna bestämmelsen, på grundval av den bestämmelsen. Enligt exempelvis de befintliga initiativen rörande intelligenta transportsystem kommer kommissionen inledningsvis att ha ett särskilt ansvar vid fastställandet av åtgärder, standardiseringsinitiativ, förfaranden och bästa metoder. ”Privacy by design” bör vara en vägledande princip vid utförandet av dessa uppgifter.

44. Europeiska datatillsynsmannen konstaterar vidare att principen om ”privacy by design” även har stor betydelse inom området med frihet, säkerhet och rättvisa, särskilt i förhållande till målen i strategin för informationshantering, enligt vad som förutses i Stockholmsprogrammet ([1]). I sitt yttrande om Stockholmsprogrammet underströk datatillsynsmannen att strukturen för informationsutbytet bör grundas på ”privacy by design” ([2]). ”Mer konkret innebär detta att informationssystem som utformas för att tillgodose allmänna säkerhetsbehov alltid ska utformas i enlighet med principen om ’privacy by design’ ”.

45. I artikel 29-arbetsgruppens yttrande om det framtida integritetsskyddet ([3]) förespråkas mer explicit att inom området med frihet, säkerhet och rättvisa – där myndigheterna är huvudaktörer och där åtgärder som ökar övervakningen direkt påverkar den grundläggande rätten till data- och integritetsskydd – bör krav på inbyggda skyddsmekanismer för personlig integritet göras obligatoriska. Genom att införa dessa krav i informationssystem skulle regeringarna dessutom stimulera ”privacy by design” i egenskap av pilotkunder.

”Privacy by design” som en vägledande princip i den digitala dagordningen för Europa

46. Informations- och kommunikationstekniken blir alltmer komplex och medför allt större risker för data- och integritetsskyddet. Rent generellt är digitaliserad information, som är lättare att få tillgång till, kopiera och överföra, exponerad för mycket högre risker än pappersbaserad information. I takt med att utvecklingen går mot nät av sammankopplade ting kommer riskerna att öka. Ju större riskerna för data- och integritetsskyddet är, desto större kommer efterfrågan på förbättrade säkerhetsmekanismer för data- och integritetsskyddet att bli. Det berättigade behovet att genomföra ”privacy by design” är följaktligen mer påtagligt inom IKT-sektorn. Dessutom, vilket diskuteras ovan, är enskilda personers förtroende för IKT avgörande för att medborgarna ska acceptera dessa nya tjänster, och data- och integritetsskyddet är nyckelfaktorer för ett sådant förtroende.

47. En utvecklingsstrategi för IKT måste följaktligen bekräfta behovet att utforma denna teknik med inbyggda mekanismer för data- och integritetsskydd, dvs. med hänsyn till principen om ”privacy by design”.

48. Den digitala dagordningen för Europa bör följaktligen uttryckligen stödja principen om ”privacy by design” som ett nödvändigt inslag för att säkerställa medborgarnas förtroende för IKT och onlinetjänster. Den bör erkänna att personlig integritet och förtroende går hand i hand, och att ”privacy by design” bör vara en vägledande faktor vid utvecklingen av en förtroendeingivande IKT-sektor.

”Privacy by design” som en princip i andra EU-initiativ

49. ”Privacy by design” bör vara en vägledande princip när kommissionen genomför politik, åtgärder och initiativ inom särskilda IKT-sektorer, inklusive e-hälsovård, e-upphandling, e-socialförsäkring, e-lärande etc. Många av dessa initiativ kommer att ingå som åtgärdspunkter i den digitala dagordningen för Europa.

50. Detta innebär till exempel att initiativ för att säkerställa mer effektiva och moderna förvaltningstillämpningar som gör det enklare för enskilda personer att interagera med förvaltningar bör inbegripa ett krav på att de utformas och drivs i enlighet med principen om ”privacy by design”. Samma sak gäller för kommissionens politik och insatser för att främja snabbare Internet, digitalt innehåll eller ett allmänt främjande av fast och trådlös kommunikation och dataöverföring.

([1]) Stockholmsprogrammet – Ett öppet och säkert Europa i medborgarnas tjänst och för deras skydd, godkänt av Europeiska rådet i december 2009.

([2]) Yttrande av den 10 juli 2009 om kommissionens meddelande till Europaparlamentet och rådet om ett område med frihet, säkerhet och rättvisa i allmänhetens tjänst, EUT C 276, 17.11.2009, s. 8, punkt 60.

([3]) Artikel 29-arbetsgruppens yttrande 168 om ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, antaget den 1 december 2009.

51. Detta omfattar även områden där kommissionen ansvarar för de storskaliga IT-systemen, t.ex. SIS och VIS, samt de fall där kommissionens ansvar är begränsat till utvecklingen och underhållet av den gemensamma infrastrukturen för sådana system, t.ex. Europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris).

52. Exakt hur principen om ”privacy by design” kommer att utvecklas kommer att vara beroende av varje enskild sektor och situation. När exempelvis kommissionens initiativ åtföljs av lagstiftningsförslag för en särskilt IKT-sektor, kommer det i flera fall att vara lämpligt att inkludera en uttrycklig hänvisning till den definition av ”privacy by design” som är tillämplig för den särskilda IKT-tillämpningen/-systemet. Om åtgärdsplaner för ett särskilt område utformas bör de systematiskt säkerställa tillämpningen av den rättsliga ramen och närmare bestämt garantera att den relevanta IKT-tekniken utvecklas med hänsyn till ”privacy by design”.

53. När det gäller forskning bör det sjunde ramprogrammet och de följande programmen användas som verktyg för att stödja projekt som syftar till att analysera standarder, IKT-teknik och IKT-arkitektur som bättre tjänar integriteten och särskilt principen om ”privacy by design”. Dessutom bör ”privacy by design” även vara ett nödvändigt inslag att överväga i bredare IKT-projekt som syftar till att behandla enskilda personers personuppgifter.

Områden av särskild vikt

54. I några fall kan det, till följd av de särskilda riskerna för enskilda personers data- och integritetsskydd eller på grund av andra faktorer (en motvilja från industrin att tillhandahålla produkter som innefattar ”privacy by design”, konsumenternas efterfrågan etc.), bli nödvändigt att mer uttryckligen och ingående definiera åtgärder för utformningen av ”privacy by design” som måste införlivas i en viss typ av informations- och kommunikationsprodukt/-teknik, eventuellt genom rättsliga instrument.

55. Europeiska datatillsynsmannen har identifierat olika områden (RFID, mötesplatser på nätet och tillämpningar via webbläsare) som enligt datatillsynsmannens åsikt i det här skedet förtjänar kommissionens noggranna övervägande och de mer praktiska ingripanden som förespråkas ovan. Dessa tre områden diskuteras mer ingående nedan.

V. **RADIOFREKVENSIDENTIFIERING – RFID**

56. RFID-taggar kan placeras i eller på föremål, djur och människor. De kan användas för att samla och lagra personuppgifter, t.ex. uppgifter i patientjournaler, att spåra och följa människors rörelser och att lägga upp profiler över deras beteenden för olika syften. Detta kan ske utan att den enskilda personen vet om det [1].

57. Ett effektivt skydd av personuppgifter, privatlivet och de därmed förbundna etiska aspekterna är avgörande för allmänhetens godtagande av radiofrekvensidentifiering och det framtida ”sakernas Internet”. Endast då kan tekniken leverera sina många ekonomiska och samhälleliga fördelar.

V.1 **Bristerna i den tillämpliga rättsliga ramen för uppgiftsskydd**

58. Dataskyddsdirektivet och direktivet om e-integritet är tillämpliga på insamlingen av data genom RFID-tillämpningar [2]. I dessa direktiv föreskrivs bland annat att tillräckliga säkerhetsåtgärder för att skydda den personliga integriteten ska införas för att driva RFID-tillämpningar [3].

59. Denna rättsliga ram behandlar emellertid inte fullt ut alla de frågor avseende data- och integritetsskyddet som denna teknik ger upphov till. Detta beror på att direktiven inte är tillräckligt detaljerade när det gäller den typ av säkerhetsskydd som bör genomföras i RFID-tillämpningar. Det är nödvändigt att komplettera de befintliga reglerna med nya

[1] RFID står för Radio Frequency Identification (radiofrekvensidentifiering). Huvudkomponenterna för RFID-teknik *eller* RFID-infrastruktur är en *tagg* (dvs. ett mikrochip), en läsare och en applikation kopplad till taggarna och läsarna genom mellanprogram och bearbetning av de framtagna uppgifterna. Själva taggarna består av en elektronisk krets som lagrar uppgifter och en antenn som överför uppgifterna via radiovågor. Läsaren har en antenn och en demodulator som översätter den inkommande analoga informationen från radiolänken till digitala uppgifter. Informationen kan sedan skickas via nätverk till databaser och servrar för att bearbetas av en dator.

[2] I direktivet om e-integritet hänvisas till RFID i artikel 3: ”Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.” Detta kompletteras genom skäl 56: ”Tekniska framsteg tillåter utvecklingen av nya tillämpningar baserade på utrustning för datainsamling och identifiering, vilket kan vara trådlös utrustning som använder radiofrekvenser. Till exempel utrustning för radiofrekvensidentifiering (RFID) använder radiofrekvenser för att fånga data från unikt identifierade taggar, som kan sändas över existerande kommunikationsnät. Den utbredda användningen av sådana tekniker kan ge avsevärda ekonomiska och sociala fördelar och därmed bidra betydelsefullt till den inre marknaden om medborgarna accepterar användningen av dem. För att uppnå detta mål är det nödvändigt att säkerställa att individernas grundläggande rättigheter, inbegripet rätten till dataskydd och integritetsskydd, garanteras. När sådan utrustning ansluts till allmänna elektroniska kommunikationsnät eller används i elektroniska kommunikationstjänster som en grundläggande infrastruktur bör de relevanta bestämmelserna i direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation), inklusive dem om säkerhet, trafik, lokaliseringsuppgifter och konfidentialitet, tillämpas.”

[3] I exempelvis artikel 17 i dataskyddsdirektivet föreskrivs en skyldighet att genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar samt otillåten spridning av uppgifterna.

som föreskriver särskilda säkerhetsskydd, och framför allt då att göra det obligatoriskt att bygga in tekniska lösningar (”privacy by design”) i RFID-teknik. Detta gäller för taggar som lagrar personuppgifter, som bör förses med ett avaktiveringskommando (ett s.k. kill command), samt användning av kryptografi i taggar som lagrar vissa typer av personuppgifter.

V.2 **Självreglering som ett första steg**

60. I mars 2007 antog kommissionen ett meddelande [1] i vilket den bland annat erkände att det kunde bli nödvändigt att ge detaljerade riktlinjer för den praktiska tillämpningen av RFID samt att det var önskvärt att anta konstruktionskriterier för att förhindra risker för privatlivet och säkerheten.

61. För att uppnå dessa mål antog kommissionen i maj 2009 en rekommendation om genomförandet av principerna om integritets- och dataskyddet i tillämpningar som stöds av radiofrekvensidentifiering (RFID) [2]. När det gäller RFID-tillämpningar som används i detaljhandeln måste taggar avaktiveras vid försäljningsstället om inte konsumenten gett sitt samtycke. Detta gäller emellertid inte om man i konsekvensanalysen avseende data- och integritetsskyddet drar slutsatsen att taggarna inte utgör ett sannolikt hot mot skyddet av privatlivet eller personuppgifter, i vilket fall de fortsätter att vara operativa efter försäljningstillfället såvida inte konsumenten väljer att taggen ska avaktiveras utan kostnad.

62. Europeiska datatillsynsmannen stöder kommissionens strategi att använda självreglerande instrument. Som ytterligare redogörs för nedan är det emellertid möjligt att de förväntade resultaten inte kommer att kunna uppnås genom självreglering, och datatillsynsmannen uppmanar därför kommissionen att vara beredd att vidta alternativa åtgärder.

V.3 **Områden av särskild vikt och eventuella ytterligare åtgärder om självreglering inte fungerar**

63. Europeiska datatillsynsmannen är bekymrad över att organisationer som driver RFID-tillämpningar inom detaljhandeln kanske överser med att RFID-taggar eventuellt kan övervakas av icke önskade tredje parter. En sådan övervakning kan avslöja personuppgifter som är lagrade på taggen (om några), men även göra det möjligt för en tredje part att följa eller känna igen en person över tiden genom att helt enkelt använda den unika identifiering som finns i en eller flera taggar som den enskilda personen har på sig, i en miljö som kanske till och med ligger utanför RFID-tillämpningens verksamhetsområde. Datatillsynsmannen hyser dessutom farhågor att operatörer av RFID-tillämpningar kan känna sig frestade att i alltför stor utsträckning förlita sig på undantaget och därmed lämna taggen operativ efter försäljningstillfället.

64. Om detta sker kanske det är för sent att minska riskerna för enskilda personers data- och integritetsskydd, som vid detta skede kanske redan har påverkats. Med tanke på självregleringens karaktär kanske dessutom nationella tillsynsmyndigheter har en svagare ställning i fråga om att ställa krav på att operatörer av RFID-tillämpningar tillämpar särskilda åtgärder för ”privacy by design”.

65. Europeiska datatillsynsmannen uppmanar därför kommissionen att, om ett effektivt genomförande av den gällande rättsliga ramen misslyckas, vara beredd att lägga fram förslag till lagstiftning som reglerar huvudfrågorna för användningen av RFID-tekniken. Kommissionens bedömning bör genomföras utan oskäligt dröjsmål. En senareläggning skulle utsätta enskilda personer för risk och även vara kontraproduktivt för branschen eftersom rättsosäkerheten är alltför hög och det sannolikt kommer att vara svårare och dyrare att korrigera djupt rotade problem.

66. Inom ramen för de åtgärdsförslag som kanske visar sig bli nödvändiga rekommenderar Europeiska datatillsynsmannen att man inför principen om frivilligt deltagande vid försäljningsstället, vilket innebär att alla RFID-taggar på konsumentprodukter automatiskt avaktiveras vid kassan. Det kanske inte skulle vara nödvändigt för kommissionen att specificera den konkreta teknik som skulle användas för detta. I stället måste EU-lagstiftningen fastställa en rättslig skyldighet att erhålla frivilligt deltagande, och låta operatörerna besluta hur detta krav ska mötas.

V.4 **Ytterligare frågor som bör övervägas: Reglering av ”sakernas Internet”**

67. Information som produceras av RFID-taggar – exempelvis produktinformation – kan så småningom eventuellt sammankopplas till ett globalt nätverk av kommunikationsinfrastruktur. Detta kallas normalt ”sakernas Internet”. Frågorna avseende data- och integritetsskyddet uppstår eftersom föremål i den verkliga världen kan identifieras genom RFID-taggar som utöver produktinformation även kan innehålla personuppgifter.

68. Det finns många öppna frågor om vem som kommer att hantera lagringen av information som rör taggade föremål. Hur kommer den att organiseras? Vem kommer att ha tillgång till denna information? I juni 2009 antog kommissionen ett meddelande om ”sakernas Internet” [3] som explicit identifierade de potentiella problem i fråga om data- och integritetsskyddet som detta fenomen kan ge upphov till.

---

[1] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén – *Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi*, 15.3.2007, KOM(2007) 96 slutlig.

[2] Kommissionens rekommendation av den 12.5.2009 om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering (RFID), (C (2009) 3200 slutlig).

[3] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *Sakernas Internet: en handlingsplan för Europa*, 18.6.2009, KOM(2009) 278 slutlig.

69. Europeiska datatillsynsmannen vill belysa några av de frågor som togs upp i detta meddelande och som enligt datatillsynsmannen måste ges stor uppmärksamhet i takt med att ”sakernas Internet” utvecklas. För det första kan behovet av decentraliserade strukturer underlätta ansvarighet samt upprätthållande av EU:s rättsliga ram. För det andra bör enskilda personers rättighet att inte bli spårade upprätthållas i möjligaste mån. Det bör med andra ord endast i begränsade fall vara möjligt att spåra människor genom RFID-taggar där de inte gett sitt medgivande. Ett sådant medgivande bör vara uttryckligt. Detta kallas normalt ”taggens tystnad” och individens rätt om att bli lämnad ifred. Slutligen bör, vid utformning av ”sakernas Internet”, principen om ”privacy by design” vara en vägledande princip. Detta skulle till exempel kräva att konkreta RFID-tillämpningar med inbyggda mekanismer som ger användarna kontroll utformas med förvalda inställningar för sekretess.

70. Europeiska datatillsynsmannen förväntar sig att bli hörd i samband med att kommissionen vidtar de åtgärder som förutses i meddelandet, särskilt under utformningen av meddelandet om personlig integritet och förtroende i det allmänt utbredda informationssamhället.

VI. MÖTESPLATSER PÅ NÄTET OCH BEHOVET AV FÖRVALDA INSTÄLLNINGAR FÖR SEKRETESS

71. Mötesplatser på nätet är ”månadens smak” och verkar i dag vara populärare än e-post. De för samman människor som delar liknande intressen och/eller aktiviteter. Människor kan lägga upp sina profiler på webben och dela med sig av sådana mediafiler som videos, foton, musik samt yrkesprofiler.

72. Ungdomar har snabbt tagit till sig mötesplatser på nätet – en trend som ökar. Den genomsnittliga åldern på Internetanvändare i Europa har sjunkit de senaste åren: I dag kopplar 9–10-åringar upp sig på nätet flera gånger i veckan och 12–14-åringar är ute på nätet varje dag, ofta i en till tre timmar.

VI.1 Mötesplatser på nätet och den tillämpliga rättsliga ramen för data- och integritetsskyddet

73. Utvecklingen av mötesplatser på nätet har gjort det möjligt för användare att lägga ut information om sig själva och tredje parter på Internet. När de gör så agerar Internetanvändare enligt artikel 29-arbetsgruppen [1] som registeransvariga i den mening som avses i artikel 2 d i dataskyddsdirektivet för de uppgifter de lägger ut [2]. I de flesta fall omfattas emellertid en sådan behandling av ”hushållsundantaget” enligt artikel 3.2 i direktivet. Samtidigt betraktas leverantörer av sociala nätverkstjänster som registeransvariga i den mån de tillhandahåller möjligheter till behandling av användaruppgifter och alla grundläggande tjänster i anslutning till användarhantering (t.ex. registrering och avslutande av konton).

74. I rättsligt hänseende innebär detta att Internetanvändare och sociala nätverkstjänster har ett gemensamt ansvar för behandlingen av personuppgifter i egenskap av ”registeransvariga” i den mening som avses i artikel 2 d i direktivet, om än i olika omfattningar och utifrån olika skyldigheter.

75. Användare bör följaktligen vara medvetna om och förstå att när de behandlar sina egna och andras personuppgifter omfattas de av bestämmelserna i EU:s lagstiftning om dataskydd som bland annat föreskriver att man måste få ett informerat samtycke från de vars uppgifter läggs upp och ge berörda personer möjlighet att utöva sin rätt till rättelse och rätten att göra invändningar etc. På samma sätt måste sociala nätverkstjänster bland annat vidta lämpliga tekniska och organisatoriska åtgärder för att hindra otillåten behandling, med hänsyn till de risker som behandlingen innebär och uppgifternas art. Sociala nätverkstjänster bör därför tillhandahålla integritetsfrämjande standardinställningar, inbegripet inställningar som begränsar åtkomsten till användarnas profilinnehåll till deras egna självvalda kontakter. Inställningarna bör också kräva användarens specifika samtycke innan något profilinnehåll görs tillgängligt för andra tredje parter, och profiler med begränsad åtkomst bör inte kunna upptäckas av interna sökmotorer.

76. Tyvärr finns det ett gap mellan de rättsliga kraven och hur de tillämpas i praktiken. Samtidigt som Internetanvändare i rättsligt hänseende betraktas som registeransvariga och är skyldiga att iaktta EU:s dataskyddsbestämmelser, är de i verkligheten ofta omedvetna om detta. De förstår i allmänhet inte att de behandlar personuppgifter eller är medvetna om de risker för data- och integritetsskyddet som är förenade med att lägga ut sådana uppgifter. Särskilt ungdomar som lägger ut innehåll på webben underskattar följderna av detta för sig själva och andra, till exempel konsekvenserna av detta senare i livet vid inskrivning vid högre utbildning eller jobbansökningar.

[1] Se artikel 29-arbetsgruppens yttrande 163, 5/2009, om sociala nätverk på Internet, antaget den 12 juni 2009.

[2] I direktivet avses med ”registeransvarig: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. När ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av gemenskapsrätten kan den registeransvarige eller de särskilda kriterierna för att utse honom anges i nationell rätt eller i gemenskapsrätten”.

77. Samtidigt tillämpar tillhandahållare av mötesplatser på nätet ofta förvalda inställningar för sekretess som grundas på s.k. opt-outs (dvs. att man själv måste ändra sina sekretessinställningar), vilket underlättare utlämnandet av personuppgifter. Vissa förvalda inställningar för sekretess gör det möjligt för t.ex. sökmotorer att komma åt personliga profiler. Detta väcker frågor om huruvida enskilda personer verkligen har gett sitt samtycke till att uppgifterna lämnas ut, samt huruvida mötesplatser på nätet har genomfört bestämmelserna i artikel 17 i direktivet (beskrivet ovan) enligt vilka de ska genomföra lämpliga tekniska och organisatoriska åtgärder för att hindra otillåten behandling.

VI.2 **Risker med mötesplatser på nätet och förslag till åtgärder för att ta itu med dessa**

78. Det ovan beskrivna leder till ökad risk för enskilda personers data- och integritetsskydd. Det utsätter Internetanvändare och enskilda personer vars personuppgifter har lagts ut för uppenbar kränkning av deras data- och integritetsskydd.

79. Kommissionen bör därför fråga sig vad som kan och måste göras för att ta itu med denna situation. Detta yttrande ger inte något uttömmande svar på den frågan utan lägger fram några förslag för vidare övervägande.

Att investera i att "utbilda" Internetanvändarna

80. Det första förslaget går ut på att investera i "utbildning" av Internetanvändarna. I detta avseende bör EU:s institutioner samt nationella myndigheter investera i att utbilda användarna och göra dem mer medvetna om de risker som är förenade med sociala nätverk på Internet. GD Informationssamhället har till exempel drivit programmet för ett säkrare Internet ("Safer Internet Programme") som syftar till att skydda barn och ungdomar som använder Internet genom bland annat projekt för att öka medvetenheten ([1]). EU:s institutioner lanserade nyligen kampanjen "Think before you post" för att öka medvetenheten om riskerna med att dela med sig av personuppgifter med främlingar.

81. Europeiska datatillsynsmannen uppmanar kommissionen att fortsätta att stödja denna typ av verksamhet. Tillhandahållare av mötesplatser på nätet bör emellertid även själva kunna spela en aktiv roll, eftersom de har ett rättsligt och socialt ansvar att upplysa användarna om hur de ska använda deras tjänster på ett säkert och integritetsfrämjande sätt.

82. Automatisk åtkomst till uppgifter som läggs ut på mötesplatser på nätet varierar alltså beroende på inställningarna för sekretess. Uppgifter kan till exempel göras tillgängliga för allmänheten i stort, inklusive sökmotorer, som kan indexera dem och därmed tillhandahålla direkta länkar till uppgifterna. Å andra sidan kan uppgifterna begränsas till "självvalda vänner" eller hållas helt privata. Tillstånden för åtkomst till profiler och den terminologi som används skiljer sig uppenbarligen från sajt till sajt.

83. Som beskrivits ovan är det emellertid inte särskilt många av de som använder sig av sociala nätverkstjänster som vet hur de ska göra för att kontrollera åtkomsten till de uppgifter de lägger ut, och framför allt inte hur de ändrar sekretessinställningarna. Dessa förblir ofta oförändrade eftersom användarna inte är medvetna om konsekvenserna av att inte ändra dem eller kanske inte vet hur man gör. I de flesta fall innebär därför det faktum att inte sekretessinställningarna ändras inte att användarna har fattat ett informerat beslut om att dela med sig av uppgifterna. I detta sammanhang är det mycket viktigt att sådana tredje parter som sökmotorer inte länkar till enskilda personers profiler under antagandet att användarna automatiskt (genom att inte ändra sekretessinställningarna) har samtyckt till att göra uppgifterna tillgängliga utan begränsningar.

84. Även om utbildning av användarna kan bidra till att ta itu med denna situation, kommer detta i sig inte vara tillräckligt. Som rekommenderas av artikel 29-arbetsgruppen i yttrandet om mötesplatser på nätet bör sociala nätverkstjänster erbjuda integritetsfrämjande och kostnadsfria standardinställningar. Detta skulle göra användare mer medvetna om vad de gör, och göra det möjligt för dem att fatta bättre beslut i fråga om huruvida de vill dela med sig av sina uppgifter och med vem.

Självregleringens roll

85. Kommissionen har undertecknat ett avtal med 20 företag som tillhandahåller mötesplatser på nätet ("Principerna om förbättrad säkerhet på mötesplatser på nätet") ([2]). Syftet med avtalet är att förbättra säkerheten för minderåriga när de använder mötesplatser på nätet i Europa. Dessa principer inkluderar flera av de krav som härleds från tillämpningen av den rättsliga ram för dataskydd som beskrivs ovan, bland annat kravet att genom verktyg och teknik säkerställa att användarna kan kontrollera hur deras personuppgifter används och sprids. Det inbegriper också behovet att tillhandahålla förvalda inställningar för sekretess.

86. I början av januari 2010 offentliggjorde kommissionen resultaten av detta i en rapport där genomförandet av principerna utvärderades ([3]). Europeiska datatillsynsmannen är bekymrad över att denna rapport visar att samtidigt som vissa åtgärder har vidtagits, har flera andra inte

([1]) Information om sådana program finns på http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Principerna finns på http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Se rapporten "Evaluation of the Implementation of the Safer Social Networking Principles for the EU" på http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

gjort det. Enligt rapporten förelåg till exempel problem med avseende på kommunikationen om de säkerhetsåtgärder och verktyg som finns tillgängliga på sajterna. Vidare konstaterades att mindre än hälften av de som undertecknat avtalet begränsade åtkomsten till minderårigas profiler till att endast omfatta deras vänner.

Behovet av obligatoriska förvalda inställningar för sekretess

87. I detta sammanhang är den avgörande frågan huruvida det är nödvändigt att vidta ytterligare politiska åtgärder för att säkerställa att mötesplatser på nätet tillhandahåller sina tjänster med förvalda inställningar för sekretess. Denna fråga togs upp av Viviane Reding, kommissionsledamot med f.d. ansvar för informationssamhället, som påpekade att det skulle kunna bli nödvändigt med lagstiftning. ([1]) I samma anda konstaterade Europeiska ekonomiska och sociala kommittén att utöver självreglering bör minimiskyddsstandarder föreskrivas i lag ([2]).

88. Som konstaterats ovan kan skyldigheten för tillhandahållare av mötesplatser på nätet att tillämpa förvalda inställningar för sekretess utläsas indirekt ur artikel 17 i dataskyddsdirektivet ([3]) enligt vilken registeransvariga måste vidta lämpliga tekniska och organisatoriska åtgärder (”både när systemet för behandlingen utformas och när själva behandlingen sker”) för att garantera säkerheten och hindra otillåten behandling, med hänsyn till de risker som behandlingen innebär och uppgifternas art.

89. Denna artikel är emellertid alldeles för allmänt formulerad och saknar närmare bestämmelser, även i detta sammanhang. Den fastställer inte uttryckligen vad som avses med lämpliga tekniska och organisatoriska åtgärder i samband med mötesplatser på nätet. Följaktligen råder för närvarande rättsosäkerhet, vilket ställer till problem för både lagstiftare och enskilda personer vars integritet och personuppgifter inte skyddas fullt ut.

90. Europeiska datatillsynsmannen uppmanar följaktligen kommissionen att utarbeta lagstiftning som åtminstone inkluderar en övergripande bestämmelse som kräver obligatoriska förvalda inställningar för sekretess, tillsammans med mer specifika krav:

a) Att tillhandahålla inställningar som begränsar åtkomsten till användarens profil till användarens självvalda kontakter. Inställningarna ska vidare kräva användarens specifika samtycke innan något profilinnehåll görs tillgängligt för tredje parter.

b) Att säkerställa att profiler med begränsad åtkomst inte kan upptäckas av interna/externa sökmotorer.

91. Förutom att föreskriva om obligatoriska förvalda inställningar för sekretess återstår frågan om det även är lämpligt med ytterligare specifikt dataskydd samt andra åtgärder (t.ex. avseende skyddet av minderåriga). Detta aktualiserar den mer allmänna frågan om det skulle vara lämpligt att skapa en särskild ram för dessa typer av tjänster som, förutom att föreskriva om obligatoriska förvalda inställningar för sekretess, skulle reglera andra aspekter. Datatillsynsmannen uppmanar kommissionen att överväga detta.

VII. FÖRVALDA INSTÄLLNINGAR FÖR SEKRETESS I WEBBLÄSARNA SOM GARANTERAR INFORMERAT SAMTYCKE ATT TA EMOT REKLAM

92. Annonsnätverk använder sig av cookies och andra verktyg för att bevaka enskilda användares beteende när de surfar på Internet i syfte att kartlägga deras intressen och skapa profiler. Denna information används sedan för att skicka riktad reklam till dem ([4]).

VII.1 Återstående utmaningar och risker inom den befintliga ramen för data- och integritetsskydd

93. Denna behandling omfattas av dataskyddsdirektivet (i den mån personuppgifter berörs) samt artikel 5.3 i direktivet om integritet och elektronisk kommunikation. I den artikeln fastställs särskilt att en användare ska informeras och ges möjlighet att reagera genom att antingen ge sitt samtycke till eller vägra att sådana anordningar som cookies etc. lagras i användarens dator eller någon annan anordning ([5]).

94. Hittills har annonsnätverk förlitat sig på webbläsarinställningar och integritetspolicys för att informera användarna och göra det möjligt för dem att acceptera eller vägra cookies. De har i sin integritetspolicy beskrivit hur man

([1]) Viviane Reding, ledamot av Europeiska kommissionen med ansvar för frågor om informationssamhället och medier: ”Think before you post! How to make social networking sites safer for children and teenagers?” Safer Internet Day Strasbourg, den 9 februari 2010.

([2]) Europeiska ekonomiska och sociala kommitténs yttrande av den 4 november 2009 om de sociala nätverkssajternas inverkan på medborgare/konsumenter.

([3]) Se även i punkt 33 i detta dokument.

([4]) En cookie är en liten textfil som innehåller en unik identifierare. Normalt placerar annonsnätverk (samt operatörer av webbsajter eller utgivare) cookies på besökarens hårddisk, framför allt på Interanvändarnas webbläsare, när användarna första gången besöker webbplatser som innehåller reklam som ingår i deras nätverk. Cookien kommer att göra det möjligt för annonsnätverket att känna igen en tidigare besökare som återvänder till webbplatsen eller besöker en webbplats som är en partner till annonsnätverk. Sådana upprepade besök kommer att göra det möjligt för annonsnätverket att skapa en profil över besökaren.

([5]) Artikel 5.3 i direktivet om e-integritet ändrades nyligen för att förstärka skyddet mot att fånga upp användarnas kommunikation genom användningen av – exempelvis – spionprogramvara och cookies som lagras på en användares dator eller annan anordning. Inom ramen för det nya direktivet bör användare erbjudas bättre information om och enklare sätt att kontrollera om de vill att cookies lagras i deras terminalutrustning.

helt väljer bort cookies alternativ accepterar dem från fall till fall. Genom att göra detta uppfyller de faktiskt sin skyldighet att ge användare rätten att vägra cookies.

95. Medan denna metod rent teoretiskt (via webbläsaren) i praktiken faktiskt skulle kunna tillhandahålla ett meningsfullt informerat samtycke förhåller det sig inte på det viset. Användarna känner i allmänhet inte alls till hur insamlingen av uppgifter fungerar, och ännu mindre insamlingen från tredje parter, inte heller värdet av sådana uppgifter, hur de används, hur tekniken fungerar eller mer närmare hur och var man stänger av cookies. De steg som användarna måste vidta för att stänga av cookies förefaller inte bara komplicerade utan även omfattande (användaren måste först ställa in sin webbläsare så att den accepterar cookies, sedan välja att stänga av dem).

96. Följaktligen väljer inte särskilt många att stänga av cookies – inte för att de har fattat ett informerat beslut att godkänna beteendestyrd annonsering, utan snarare eftersom de inte inser att de genom att inte välja att stänga av dem accepterar cookies.

97. Även om artikel 5.3 i direktivet om e-integritet därför i rättsligt hänseende ger ett effektivt skydd, tvingas Internetanvändare i praktiken att samtycka till att övervakas när det gäller att skicka beteendestyrd reklam även om de i själva verket i många, om inte alla, fall är helt omedvetna om den övervakning som sker.

98. Artikel 29-arbetsgruppen håller på att utarbeta ett yttrande som syftar till att klargöra de rättsliga krav som råder för beteendestyrd annonsering, vilket välkomnas. En tolkning kanske emellertid inte är tillräckligt för att lösa denna situation och det kanske blir nödvändigt för Europeiska unionen att vidta ytterligare åtgärder.

VII.2 **Behov av ytterligare åtgärder, framför allt bestämmelser om obligatoriska förvalda inställningar för sekretess**

99. Som beskrivits ovan tillåter webbläsare normalt kontroll över vissa typer av cookies. De flesta webbläsare har en förvald inställning som gör att de accepterar alla cookies. En webbläsares förvalda inställningar tillåter med andra ord alla cookies oavsett syftet. För att förhindra cookies måste användaren alltså ändra inställningarna på sin webbläsare, vilket enligt vad som angetts ovan väldigt få användare gör. Dessutom finns det ingen guide (*wizard*) för sekretessinställningar vid den första installationen eller vid uppdateringar av webbläsartillämpningar.

100. Ett sätt att minska detta problem skulle vara att förse webbläsaren med förvalda inställningar för sekretess. Den skulle följaktligen vara inställd på ”accepterar inte cookies från tredje parter”. För att komplettera detta och göra det mer effektivt skulle webbläsaren kräva att användarna använde en guide för sekretessinställningar när de för första gången installerar eller när de uppdaterar webbläsaren. Det finns ett behov av mer detaljerad och tydlig information om de olika typerna av cookies och fördelarna med några av dem. De användare som är villiga att låta sig övervakas i syfte att ta emot reklam skulle i vederbörlig ordning informeras om detta och skulle behöva ändra sina webbläsarinställningar. Detta skulle ge dem ökad kontroll över sina personuppgifter och sin personliga integritet och skulle, enligt Europeiska datatillsynsmannen, vara ett effektivt sätt att respektera och värna om användarnas samtycke ([1]).

101. Med hänsyn till å ena sidan omfattningen av detta problem, dvs. det stora antal Internetanvändare som för närvarande övervakas på grundval av ett illusoriskt samtycke och, å andra sidan, de mer omfattande intressen som står på spel, blir behovet av ytterligare säkerställande åtgärder mer akut. Genomförandet av principen om ”privacy by design” i webbläsartillämpningar skulle kunna göra en mycket stor skillnad när det gäller att ge enskilda personer kontroll över de förfaranden som tillämpas för att samla in uppgifter för annonseringsändamål.

102. Europeiska datatillsynsmannen uppmanar därför kommissionen att överväga rättsliga åtgärder som kräver obligatoriska förvalda inställningar för sekretess på webbläsare och tillhandahållande av relevant information.

VIII. **ANDRA PRINCIPER SOM SYFTAR TILL ATT SKYDDA ENSKILDA PERSONERS DATA- OCH INTEGRITETSSKYDD**

103. Samtidigt som principen om ”privacy by design” har stor potential att förbättra enskilda personers data- och integritetsskydd är det nödvändigt att i lag utforma och genomföra kompletterande principer för att säkerställa konsumenternas förtroende för IKT. Mot denna bakgrund tar Europeiska datatillsynsmannen upp principen om ansvarighet och färdigställandet av ett obligatoriskt regelverk för säkerhetsöverträdelser som skulle vara tillämpligt inom alla sektorer.

VIII.1 **Principen om ansvarighet för att säkerställa iakttagande av principen om ”privacy by design”**

104. I artikel 29-arbetsgruppens yttrande om ”The Future of Privacy” ([2]) rekommenderas att principen om ansvarighet

([1]) Datatillsynsmannen är samtidigt medveten om att detta inte helt skulle lösa problemet eftersom det finns cookies som inte går att kontrollera genom webbläsaren, t.ex. s.k. flash cookies. För att komma till bukt med detta skulle det krävas att utvecklare av webbläsare ser till att kontroller över flash cookies finns integrerade i deras kontroller över cookies redan när nya webbläsare släpps ut på marknaden.

([2]) Artikel 29-arbetsgrupens yttrande 168 om ”The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, antaget den 1 december 2009.

införlivas i dataskyddsdirektivet. Denna princip, som erkänns i vissa multinationella instrument för dataskydd ([1]), kräver att organisationer genomför förfaranden för att iaktta gällande lagar samt inför metoder för att bedöma och påvisa överensstämmelse med lagar och andra bindande instrument.

105. Europeiska datatillsynsmannen stöder fullt ut artikel 29-arbetsgruppens rekommendation. Datatillsynsmannen anser att denna princip kommer att vara mycket relevant för att främja en effektiv tillämpning av principer och skyldigheter med avseende på dataskydd. Ansvarighet kommer att kräva att registeransvariga visar att de har infört de mekanismer som krävs för att iaktta tillämplig dataskyddslagstiftning. Detta kommer sannolikt att bidra till ett effektivt genomförande av principen om ”privacy by design” i IKT som ett i synnerhet lämpligt inslag för att påvisa ansvarighet.

106. För att mäta och påvisa ansvarighet skulle registeransvariga kunna använda interna förfaranden samt anlita tredje parter som skulle kunna utföra revisioner eller andra typer av kontroller och verifikationer och till följd av dessa utfärda märkning eller utmärkelser. I detta sammanhang uppmanar Europeiska datatillsynsmannen med kraft kommissionen att överväga huruvida, utöver en allmän ansvarighetsprincip, det skulle kunna vara värdefullt att i lag fastställa särskilda ansvarighetsåtgärder, exempelvis behovet att utarbeta konsekvensanalyser för data- och integritetsskyddet och under vilka omständigheter.

VIII.2 **Säkerhetsöverträdelse: att färdigställa den rättsliga ramen**

107. Genom de ändringar av direktivet om e-integritet och som genomfördes förra året infördes ett krav att anmäla personuppgiftsbrott till de enskilda personer som påverkas samt till de berörda myndigheterna. Ett personuppgiftsbrott definieras generellt som ett brott som leder till utplåning, förlust, avslöjande etc. av personuppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av tjänsten. Om personuppgiftsbrottet kan antas inverka menligt på en enskild persons personuppgifter eller integritet måste den enskilda personen underrättas om detta brott. Detta kan vara fallet om brottet skulle kunna medföra identitetsstöld eller betydande förnedring eller skadat rykte. Vid ett personuppgiftsbrott föreligger en skyldighet att anmäla detta till de behöriga myndigheterna, oavsett om det föreligger en risk för enskilda personer.

Att tillämpa skyldigheter i fråga om säkerhetsöverträdelser inom alla sektorer

108. Tyvärr gäller denna skyldighet endast för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster, t.ex. telefonbolag, Internetleverantörer, e-postleverantörer etc. Europeiska datatillsynsmannen uppmanar kommissionen att lägga fram förslag om säkerhetsöverträdelser som är tillämpliga inom alla sektorer. När det gäller innehållet i ett sådant regelverk anser Europeiska datatillsynsmannen att den rättsliga ram för säkerhetsöverträdelser som antagits i direktivet om e-integritet garanterar en tillräcklig balans mellan skyddet av enskilda personers rättigheter, däribland deras rättigheter avseende personuppgifter och integritet, och skyldigheterna för de enheter som omfattas. Denna rättsliga ram är dessutom långtifrån tandlös eftersom den backas upp av meningsfulla genomförandebestämmelser som ger myndigheterna tillräckliga befogenheter att undersöka och införa påföljder i fall av bristande efterlevnad.

109. Europeiska datatillsynsmannen uppmanar därför kommissionen att anta ett lagstiftningsförslag för att tillämpa denna ram inom alla sektorer, vid behov med nödvändiga anpassningar. Detta skulle dessutom säkerställa att samma standarder och förfaranden tillämpades inom alla sektorer.

Att genom kommittéförfaranden fullgöra den rättsliga ram som finns i direktivet om integritet och elektronisk kommunikation

110. Det reviderade direktivet om e-integritet ger kommissionen rätt att anta tekniska genomförandeåtgärder, dvs. detaljerade åtgärder som rör anmälningar av säkerhetsöverträdelser, genom ett kommittéförfarande. ([2]) Denna befogenhet är berättigad för att säkerställa ett konsekvent genomförande och tillämpning av den rättsliga ramen för säkerhetsöverträdelse. Ett konsekvent genomförande bidrar till att ge enskilda personer i hela gemenskapen samma höga skyddsnivå och till att de enheter som omfattas inte belastas med olika anmälningskrav.

111. Direktivet om e-integritet antogs i november 2009. Det tycks inte finnas någon anledning att skjuta upp inledandet av arbetet för att anta de tekniska genomförandeåtgärderna. Europeiska datatillsynsmannen har organiserat två seminarier som syftade till att dela med sig av och samla in erfarenheter om anmälningar av överträdelser av dataskyddet. Datatillsynsmannen skulle med glädje dela med sig resultaten av dessa seminarier och ser fram mot att arbeta tillsammans med kommissionen och andra berörda parter för att finjustera den övergripande rättsliga ramen för personuppgiftsbrott.

112. Europeiska datatillsynsmannen uppmanar kommissionen att inom kort vidta de åtgärder som krävs. Innan tekniska genomförandeåtgärder antas måste kommissionen genomföra ett omfattande samråd med deltagande av Europeiska byrån för nät- och informationssäkerhet (Enisa), Europeiska datatillsynsmannen och artikel 29-arbetsgruppen. Detta samråd måste dessutom inbegripa andra ”berörda parter”, framför allt för att få information om bästa tillgängliga tekniska och ekonomiska medel för genomförandet.

([1]) OECD:s riktlinjer från 1980 om integritetsskydd och persondataflöde; Madrid Privacy Declaration on Global Privacy Standards for a Global World, av den 3 november 2009.

([2]) Kommittéförfaranden innebär att tekniska genomförandeåtgärder antas av en kommitté som består av företrädare för medlemsstaterna och som har en företrädare för kommissionen som ordförande. När det gäller direktivet om e-integritet är det s.k. förfarandet med kontroll tillämpligt, vilket innebär att Europaparlamentet, samt rådet, kan motsätta sig förslag till åtgärder som kommissionen lägger fram. Se även http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **SLUTSATSER**

113. Förtroende, eller snarare bristen på förtroende, har identifierats som en huvudfråga i uppkomsten och en framgångsrik användning av informations- och kommunikationsteknik. Om människor inte har förtroende för IKT kommer denna teknik med all sannolikhet att misslyckas. Ett förtroende för IKT är beroende av flera olika faktorer varav en nyckelfaktor är att se till att en sådan teknik inte urholkar enskilda personer grundläggande rätt till integritets- och personuppgiftsskydd.

114. För att ytterligare stärka den rättsliga ramen för data- och integritetsskydd, vars principer förblir fullständigt giltiga i informationssamhället, föreslår Europeiska datatillsynsmannen att kommissionen införlivar ”privacy by design” på olika lagstiftningsnivåer och nivåer i beslutsfattandet.

115. Datatillsynsmannen rekommenderar att kommissionen följer fyra handlingslinjer:

a) Att lägga fram ett förslag som inkluderar en allmän bestämmelse om ”privacy by design” i den rättsliga ramen för dataskydd. Denna bestämmelse skulle vara teknikneutral och iakttagelse skulle vara obligatoriskt i olika stadier.

b) Att vidareutveckla denna allmänna bestämmelse i särskilda bestämmelser i samband med att förslag till särskilda rättsliga instrument för olika sektorer läggs fram. Dessa särskilda bestämmelser skulle redan nu kunna inkluderas i rättsliga instrument, på grundval av artikel 17 i dataskyddsdirektivet (och annan befintlig lagstiftning).

c) Att inkludera ”privacy by design” som en vägledande princip i den digitala dagordningen för Europa.

d) Att införa ”privacy by design” som en princip i andra EU-initiativ (främst icke lagstiftande).

116. Inom tre särskilda IKT-områden rekommenderar Europeiska datatillsynsmannen att kommissionen utvärderar behovet att lägga fram förslag som genomför principen om ”privacy by design” på olika sätt:

a) På området för RFID: att, om ett effektivt genomförande av den gällande rättsliga ramen misslyckas, lägga fram förslag till rättsliga åtgärder som reglerar huvudfrågorna för användningen av RFID-tekniken. Att i synnerhet införa principen om frivilligt deltagande vid försäljningsstället, vilket innebär att alla RFID-taggar på konsumentprodukter automatiskt skulle avaktiveras vid kassan.

b) På området för mötesplatser på nätet: att utarbeta lagstiftning som åtminstone inkluderar en övergripande bestämmelse som kräver obligatoriska förvalda inställningar för sekretess, tillsammans med mer specifika krav som begränsar åtkomsten till användarens profil till användarens självvalda kontakter samt säkerställer att profiler med begränsad åtkomst inte kan upptäckas av interna/externa sökmotorer.

c) På området för riktad reklam: att överväga lagstiftning som gör det obligatoriskt med förvalda inställningar på webbläsaren som vägrar cookies från tredje parter och som kräver att användarna använder en inställningsguide när de första gången installerar eller när de uppdaterar webbläsaren.

117. Slutligen uppmanar Europeiska datatillsynsmannen att kommissionen:

a) överväger att införliva principen om ansvarighet i det befintliga dataskyddsdirektivet, och

b) utvecklar ett regelverk av regler och förfaranden för att genomföra bestämmelserna om anmälningar av säkerhetsöverträdelser i direktivet om e-integritet, och att utvidga dem så att de gäller generellt för alla registeransvariga.

Utfärdat i Bryssel den 18 mars 2010.

Peter HUSTINX

Europeiska datatillsynsmannen