I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om styrkelse af tilliden til informationssamfundet ved at fremme databeskyttelse og privatlivets fred

(2010/C 280/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlige artikel 16,

under henvisning til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 7 og 8,

under henvisning til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([1]),

under henvisning til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor ([2]),

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ([3]), særlig artikel 41 —

VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. Informations- og kommunikationsteknologier (ikt) åbner kolossale muligheder i praktisk talt alle aspekter at vort liv — hvordan vi arbejder, leger og socialiserer og uddanner os. De er afgørende for dagens informationsøkonomi og for samfundet overordnet set.

2. Den Europæiske Union gør sig på globalt plan gældende inden for avanceret ikt og er fast besluttet på at fastholde denne position. For at tage denne udfordring op forventes Europa-Kommissionen snart at vedtage en ny digital dagsorden for Europa, hvilket kommissær Kroes har bekræftet som sin prioritet ([4]).

3. EDPS erkender de fordele, der er forbundet med ikt, og er enig i, at EU bør gøre sit yderste for at fremhjælpe udviklingen og den generelle anvendelse heraf. EDPS støtter ligeledes fuldt ud de synspunkter, som kommissær Kroes og kommissær Reding har givet udtryk for med hensyn til, at enkeltpersoner bør være i centrum i denne nye kontekst ([5]). Enkeltpersoner bør være i stand til at stole på, at ikt kan værne om deres oplysninger, og kontrollere anvendelsen heraf samt have tillid til, at der værnes om deres ret til privatlivs- og databeskyttelse i den digitale tidsalder. Det er vigtigt at respektere disse rettigheder for at skabe forbrugertillid. Og en sådan tillid er af afgørende betydning, hvis borgerne skal tage nye tjenester til sig ([6]).

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

([4]) Svar på spørgeskema fra Europa-Parlamentet til kommissær Neelie Kroes i forbindelse med Europa-Parlamentets høringer forud for udnævnelsen af kommissæren.
([5]) Svar på spørgeskema fra Europa-Parlamentet til kommissær Neelie Kroes i forbindelse med Europa-Parlamentets høringer forud for udnævnelsen af kommissæren; kommissær Viviane Redings tale om »En europæisk digital dagsorden for den nye digitale forbruger«, holdt på BEUC multi-forum om »Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives« (forbrugernes ret til privatlivets fred og onlinemarkedsføring: markedstendenser og politiske perspektiver), Bruxelles, 12. november 2009.
([6]) Se f.eks. rapport fra RISEPTIS, »Trust in the Information Society«, A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society). Findes på http://www.think-trust.eu/general/news-events/riseptis-report.html. Se også: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. EU har en stærk lovgivningsramme for databeskyttelse/privatlivets fred, hvis principper fortsat er fuldt ud relevante i den digitale tidsalder. Man kan dog ikke tillade sig at læne sig tilbage. I mange tilfælde rejser ikt nye problemstillinger, der ikke er taget højde for inden for den eksisterende ramme. Der er derfor behov for en række foranstaltninger for at sikre, at de individuelle rettigheder, der er nedfældet i EU-retten, fortsat giver en effektiv beskyttelse i denne nye kontekst.

5. I denne udtalelse behandles foranstaltninger, som enten kan fremmes eller gennemføres af Den Europæiske Union for at garantere privatlivs- og databeskyttelsen for enkeltpersoner i en globaliseret verden, som vil forblive teknologistyret. Både lovgivnings- og ikke-lovgivningsinstrumenter vil blive taget op.

6. Efter en oversigt, der viser ikt som en ny udvikling, der skaber muligheder, men også risici, behandles behovet for på praktisk plan at integrere databeskyttelse og privatlivets fred helt fra starten af nye informations- og kommunikationsteknologier (omtalt som »privacy by design«-princippet (»indbygget databeskyttelse«)). For at gennemtvinge overholdelse af dette princip ses der i udtalelsen nærmere på behovet for at indføre »privacy by design«-princippet i lovgivningsrammen for databeskyttelse på mindst to forskellige måder. For det første ved at indarbejde det som et generelt bindende princip og for det andet ved at indarbejde det på særlige ikt-områder, hvor der er specifikke risici for databeskyttelsen/privatlivets fred, der kan mindskes ved hjælp af en hensigtsmæssig teknisk arkitektur og udformning. Disse områder er radiofrekvensbaseret identifikation (RFID), sociale netværksapplikationer og browserapplikationer. Endelig stilles der i udtalelsen forslag vedrørende andre redskaber og principper, der har til formål at værne om privatlivets fred og databeskyttelsen i ikt-sektoren.

7. Ved behandlingen af ovennævnte uddybes nogle af de bemærkninger, som Artikel 29-Gruppen anførte i sit bidrag til den offentlige høring om fremtiden for privatlivets fred ([1]). Udtalelsen bygger endvidere på tidligere udtalelser fra EDPS, f.eks. udtalelsen af 25. juli om gennemførelsen af databeskyttelsesdirektivet, udtalelsen af 20. december 2007 om RFID og EDPS' to udtalelser om e-databeskyttelsesdirektivet ([2]).

II. IKT SKABER NYE MULIGHEDER, MEN OGSÅ NYE RISICI

8. Ikt er blevet sammenlignet med andre vigtige opfindelser tidligere, f.eks. elektricitet. Selv om det måske er for tidligt at vurdere de reelle historiske virkninger heraf, er der en klar forbindelse mellem ikt og økonomisk vækst i de udviklede lande. Ikt har skabt arbejdspladser og økonomiske fordele og har bidraget til den generelle velfærd. Virkningen er mere end rent økonomisk, da ikt har spillet en vigtig rolle med hensyn til at styrke innovation og kreativitet.

9. Desuden har ikt ændret den måde, hvorpå folk arbejder, socialiserer sig og interagerer. F.eks. anvender borgerne i stigende grad ikt til sociale og økonomiske interaktioner. Enkeltpersoner kan udnytte en lang række nye ikt-applikationer som f.eks. e-sundhed, e-transport, e-forvaltning og innovative interaktive systemer til underholdning og læring.

10. I lyset af sådanne fordele har EU-institutionerne alle udtrykt deres engagement i at støtte ikt som et nødvendigt redskab til at forbedre den europæiske industris konkurrenceevne og fremskynde den økonomiske genopretning i Europa. I august 2009 vedtog Kommissionen således rapporten om EU's digitale konkurrenceevne ([3]) og lancerede en offentlig høring om hensigtsmæssige fremtidige strategier til at fremme ikt. Den 7. december 2009 fremlagde Rådet et bidrag til denne høring med titlen »Post i2010-strategien mod et åbent, grønt og konkurrencedygtigt vidensamfund« ([4]). Europa-Parlamentet

([1]) Artikel 29-Gruppen, udtalelse 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« (fremtiden for privatlivets fred, fælles bidrag til Europa-Kommissionens høring om den retlige ramme for den grundlæggende ret til beskyttelse af personoplysninger), vedtaget den 1. december 2009.

([2]) Udtalelse af 25. juli 2007 om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet, EUT C 255 af 27.10.2007, s. 1; udtalelse af 20. december 2007 om meddelelsen fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme, KOM(2007) 96, EUT C 101 af 23.4.2008, s. 1; udtalelse af 10. april 2008 om forslag til direktiv om ændring af bl.a. direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), EUT C 181 af 18.7.2008, s. 1; anden udtalelse af 9. januar 2009 om revisionen af direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

([3]) Rapport om EU's digitale konkurrenceevne — Hovedresultater af i2010-strategien 2005-2009, (SEC (2009) 1060).

([4]) Rådets konklusioner »Post i2010-strategien mod et åbent, grønt og konkurrencedygtigt vidensamfund«, (17107/09), vedtaget den 18.12.2009.

har netop vedtaget en betænkning, som er tænkt som vejledning for Kommissionen ved definitionen af en digital dagsorden ([1]).

11. Sammen med de muligheder og fordele, der ledsager udviklingen af ikt, kommer nye risici, navnlig for privatlivets fred og beskyttelsen af personoplysninger med hensyn til enkeltpersoner. Ikt fører ofte til formering (meget ofte på måder, som er ude af syne for den enkelte) med hensyn til de mængder af oplysninger, der indsamles, sorteres, filtreres, overføres eller på anden måde tilbageholdes, og der er derfor mangfoldige risici for sådanne data.

12. F.eks. erstatter RFID-chips stregkoder på (nogle) forbrugsvarer. Ved at forbedre informationsstrømmen i forsyningskæden (og derved reducere behovet for »sikkerhedslagre«, fremlægge mere præcise skøn osv.) skal det nye system være en fordel for både erhvervslivet og forbrugerne. Dette er imidlertid samtidig forbundet med den foruroligende mulighed for, at man til forskellige formål og af forskellige enheder kan blive sporet via mærkede personlige ejendele.

13. Et andet eksempel er »cloud computing«, hvilket i det væsentlige er levering af hostede forbruger- og ikke-forbrugerapplikationstjenester over internettet. Der er her tale om en række forskellige tjenester lige fra fotobiblioteker, kalendere, webmail og kundedatabaser til mere komplekse erhvervsrelaterede tjenester. Fordelene for både virksomheder og enkeltpersoner er klare: nedbringelse af omkostningerne (omkostningerne er gradvis stigende), stedsuafhængighed (let adgang til oplysninger overalt i verden), automatisering (intet behov for dedikerede it-ressourcer og for at holde software opdateret) osv. Samtidig forekommer der sikkerhedsbrist og hacking som meget reelle fænomener. Der er også problemstillingen med hensyn til, at man kan miste adgangen til og kontrollen med sine egne data.

14. Fordele og risici har vist sig at være til stede på samme tid på andre områder, hvor der anvendes ikt-applikationer. Som et eksempel kan nævnes e-sundhed, der kan øge effektiviteten, nedbringe omkostningerne, øge tilgængeligheden og generelt forbedre sundhedstjenesternes kvalitet. E-sundhed rejser imidlertid ofte spørgsmålet om lovligheden af sekundære anvendelser af e-sundhedsoplysninger, hvilket kræver en nøje analyse af formålet med enhver potentiel sekundær anvendelse ([2]). Efterhånden som anvendelsen af elektroniske patientjournaler er blevet udbredt, har systemerne selv desuden været ramt af skandaler, hvor der blev afsløret mange tilfælde af hacking ind i elektroniske patientjournaler.

15. Sammenfattende vil der formentlig fortsat være et vist omfang af resterende risiko, selv når man har foretaget de rigtige vurderinger og iværksat de nødvendige foranstaltninger. En situation med nulrisiko vil være urealistisk. Som det behandles nedenfor, kan og skal der imidlertid gennemføres foranstaltninger for at mindske en sådan risiko til acceptable niveauer.

III. »PRIVACY BY DESIGN« SOM ET VIGTIGT REDSKAB TIL AT SKABE INDIVIDUEL TILLID TIL IKT

16. De potentielle fordele ved ikt kan kun opnås i praksis, hvis disse teknologier er i stand til at skabe tillid, dvs. hvis de kan sikre, at brugerne er rede til at anvende ikt på grund af egenskaberne og fordelene herved. En sådan tillid vil kun blive skabt, hvis teknologierne er pålidelige, sikre, under enkeltpersoners kontrol, og hvis beskyttelsen af deres personoplysninger og privatlivets fred er garanteret.

17. Udbredte risici og fejl som dem, der er beskrevet ovenfor, navnlig når de indebærer misbrug eller brud på datasikkerheden, hvor oplysninger om enkeltpersoners privatliv afsløres, vil sandsynligvis bringe brugertilliden i fare i informationssamfundet. Dette kunne alvorligt sætte udviklingen af ikt og de fordele, der kan opnås derved, over styr.

18. Løsningen på disse risici for privatlivs- og databeskyttelsen kan imidlertid ikke være at undlade eller afvise at anvende eller fremme ikt. Dette vil hverken være gennemførligt eller realistisk; det vil afskære enkeltpersoner fra at få fordelene ved ikt og alvorligt begrænse de generelle fordele, der kan opnås.

19. EDPS er af den opfattelse, at det er en mere positiv løsning at udforme og udvikle ikt på en måde, der respekterer privatlivs- og databeskyttelsen. Det er derfor af afgørende betydning, at privatlivs- og databeskyttelsen indgår som en fast bestanddel i hele teknologiens livscyklus, lige fra den allertidligste designfase til den endelige ibrugtagning, anvendelse og endelige bortskaffelse. Dette omtales normalt som »privacy by design« og behandles nærmere nedenfor.

20. »Privacy by design« kan omfatte forskellige tiltag, afhængigt af det specifikke tilfælde eller den specifikke applikation. F.eks. kan det i nogle tilfælde være nødvendigt at fjerne eller reducere personoplysninger eller forhindre unødvendig og/eller uønsket behandling. I andre tilfælde kan »privacy by design« være i form af redskaber, der kan øge enkeltpersoners kontrol med deres personoplysninger.

([1]) Betænkning om udformning af en ny digital dagsorden for Europa: fra i2010 til digital.eu, (2009/2225 (INI)), vedtaget den 18.3.2010.

([2]) F.eks. vil salg eller anvendelse af sundhedsoplysninger, der er indsamlet i behandlingsøjemed, og som ikke må anvendes til at udvælge steder til satellitklinikker, til at etablere ambulante kirurgicentre og til på andre måder at planlægge fremtidige aktiviteter med finansielle følger, kræve en nøje undersøgelse.

Sådanne foranstaltninger bør overvejes, når standarder og/eller bedste praksis defineres. De kan også indbygges i informations- og kommunikationssystemernes arkitektur eller i den strukturelle organisation i de enheder, der behandler personoplysninger.

III.1. **Anvendelse af »privacy by design«-princippet i forskellige ikt-miljøer og virkningen heraf**

21. Behovet for »privacy by design«-princippet findes i mange forskellig ikt-miljøer. F.eks. anvendes i sundhedssektoren i stigende grad ikt-infrastrukturer, hvor der ofte forekommer central lagring af helbredsrelaterede oplysninger om patienter. For at anvende »privacy by design«-princippet i sundhedssektoren skal det vurderes, om forskellige foranstaltninger er egnede, f.eks. muligheden for at minimere mængden af data, der lagres centralt, eller begrænse det til et indeks, anvende krypteringsværktøjer, tildele adgangsrettigheder kun til »det absolut påkrævede«, anonymisere data, når der ikke længere er behov for dem, osv.

22. Ligeledes har transportsystemer i stigende grad som standard avancerede ikt-applikationer, der interagerer med køretøjet og dets miljø til forskellige formål og funktioner. F.eks. er biler i stigende grad udstyret med ny ikt-funktionalitet (GPS, GSM, sensornet osv.), som ikke kun viser deres position, men også deres tekniske tilstand i realtid. Disse oplysninger kan anvendes til f.eks. at erstatte det eksisterende vejskatsystem med en brugsafhængig vejafgift. Anvendelsen af »privacy by design« på udformningen af en sådan systemarkitektur bør understøtte behandlingen og den videre overførsel af så få personoplysninger som muligt ([1]). I overensstemmelse med dette princip vil decentraliserede eller delvist decentraliserede arkitekturer, der begrænser videregivelsen af lokaliseringsdata til et centralt punkt, være at foretrække frem for centraliserede arkitekturer.

23. Ovennævnte eksempler viser, at når informations- og kommunikationsteknologier udformes i overensstemmelse med »privacy by design«-princippet, kan risiciene for privatlivs- og databeskyttelsen minimeres betydeligt.

III.2. **Utilstrækkelig ibrugtagning af ikt, der anvender »privacy by design«**

24. Det er et vigtigt spørgsmål, om økonomiske aktører, ikt-producenter/-leverandører og registeransvarlige er interesseret i at markedsføre og gennemføre »privacy by design«-princippet i ikt. I denne forbindelse er det også vigtigt at vurdere brugernes efterspørgsel efter »privacy by design«.

25. I 2007 offentliggjorde Kommissionen en meddelelse, hvori virksomhederne blev opfordret til at udnytte deres innovationsevne til at skabe og gennemføre teknologier til beskyttelse af privatlivet som en måde til at forbedre beskyttelsen af privatlivet og personoplysninger helt fra starten af udviklingscyklussen ([2]).

26. De foreliggende data viser imidlertid indtil videre, at det hverken er lykkedes ikt-producenter eller registeransvarlige (i den private eller offentlige sektor) konsekvent at gennemføre eller markedsføre »privacy by design«. Der er anført forskellige begrundelser herfor, herunder manglende økonomiske incitamenter eller institutionel støtte, utilstrækkelig efterspørgsel osv. ([3]).

27. Samtidig har brugernes efterspørgsel efter »privacy by design« været ret lav. Brugere af ikt-produkter og -tjenester kan med rette antage, at deres privatliv og personoplysninger rent faktisk er beskyttet, når de i mange tilfælde ikke er det. I nogle tilfælde er de ganske enkelt ikke i stand til at træffe de sikkerhedsforanstaltninger, der er nødvendige for at beskytte enten deres egne eller andres personoplysninger. I mange tilfælde skyldes dette, at de mangler fuldt eller endog delvist kendskab til risiciene. F.eks. lader unge generelt set hånt om de risici for privatlivets fred, der er forbundet med at vise personoplysninger på sociale netværk, og ignorerer ofte privatlivsindstillinger. Andre brugere er klar over risiciene, men har måske ikke den nødvendige tekniske ekspertise til at gennemføre sikkerhedsteknologier, f.eks. teknologier, der beskytter internetforbindelsen, eller viden om, hvordan browserindstillingerne ændres for at minimere den profilering, der sker på grundlag af overvågningen af deres surfingaktiviteter på internettet.

28. Alligevel er risiciene for privatlivs- og databeskyttelsen meget reelle. Hvis der ikke tages hensyn til privatlivs- og databeskyttelsen fra starten, er det ofte for sent og for økonomisk byrdefuldt at rette op på systemerne og for

([1]) Se udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 22. juli 2009 om Kommissionens meddelelse om en handlingsplan for udbygning af intelligente transportsystemer i Europa og det ledsagende forslag til Europa-Parlamentets og Rådets direktiv om fastlæggelse af rammerne for ibrugtagning af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportmåder, findes på: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Meddelelse af 2.5.2007. KOM(2007) 228 endelig fra Kommissionen til Europa-Parlamentet og Rådet om bedre databeskyttelse med teknologier til beskyttelse af privatlivet.

([3]) »Study on the economic benefits of privacy enhancing technologies (PETS)« (undersøgelse af de økonomiske fordele ved teknologier til beskyttelse af privatlivet), jls/2008/D4/036.

sent at afhjælpe den skade, der allerede er gjort. Det stigende antal brud på datasikkerheden i de senere år illustrerer præcist dette problem og understreger behovet for »privacy by design«.

29. Det fremgår klart af ovenstående, at producenter og leverandører af ikt-teknologier, der er udformet til at behandle personoplysninger, sammen med de registeransvarlige bør have ansvaret for at udforme dem med indbyggede foranstaltninger til data- og privatlivsbeskyttelse. I mange tilfælde indebærer dette, at de skal udformes med privatlivsvenlige standardindstillinger.

30. På denne baggrund bør vi overveje, hvilke foranstaltninger de politiske beslutningstagere bør træffe for at fremme »privacy by design« i udviklingen af ikt. Et første spørgsmål er, om den eksisterende lovgivningsramme for databeskyttelse indeholder tilstrækkelige bestemmelser til at sikre, at både registeransvarlige og producenter/udviklere gennemfører »privacy by design«-princippet. Et andet spørgsmål er, hvad der bør gøres i forbindelse med den digitale dagsorden for Europa for at sikre, at iktsektoren skaber forbrugertillid.

IV. INTEGRERING AF »PRIVACY BY DESIGN«-PRINCIPPET I EU'S LOVGIVNING OG POLITIKKER

IV.1. Den nuværende lovgivningsramme for databeskyttelse og privatlivets fred

31. EU har en solid lovgivningsramme for databeskyttelse og privatlivets fred i direktiv 95/46/EF ([1]), direktiv 2002/58/EF ([2]) og Den Europæiske Menneskerettighedsdomstols ([3]) og Domstolens retspraksis.

32. Databeskyttelsesdirektivet finder anvendelse på »enhver operation eller række af operationer […] som personoplysninger gøres til genstand for« (indsamling, opbevaring, videregivelse osv.). I henhold til direktivet skal de personer, der behandler personoplysninger (»registeransvarlige«), overholde visse principper og forpligtelser. Det fastsætter individuelle rettigheder, f.eks. retten til at få adgang til personoplysninger. I e-databeskyttelsesdirektivet behandles specifikt beskyttelsen af privatlivets fred i den elektroniske kommunikationssektor ([4]).

33. Det nuværende databeskyttelsesdirektiv indeholder ikke et udtrykkeligt krav om »privacy by design«. Det indeholder imidlertid bestemmelser, som i forskellige situationer indirekte kan kræve, at »privacy by design«-princippet gennemføres. I henhold til artikel 17 skal registeransvarlige således iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at forhindre ulovlig behandling ([5]). »Privacy by design« er derfor omfattet meget generelt. Desuden er direktivets bestemmelser hovedsagelig rettet til registeransvarlige og deres behandling af personoplysninger. De kræver ikke udtrykkeligt, at informations- og kommunikationsteknologier skal sikre privatlivs- og databeskyttelse, hvilket nødvendiggør, at designere og producenter af ikt også omfattes, herunder også aktiviteterne i standardiseringsfasen.

34. E-databeskyttelsesdirektivet er mere eksplicit. Det hedder i artikel 14, stk. 3: »Hvor der er behov herfor, kan der vedtages foranstaltninger for at sikre, at terminaludstyr fremstilles på en måde, der er forenelig med brugernes ret til at beskytte og kontrollere anvendelsen af deres personoplysninger i overensstemmelse med direktiv 1999/5/EF og Rådets beslutning 87/95/EØF af 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation«. Denne bestemmelse er imidlertid aldrig blevet anvendt ([6]).

35. Mens de ovennævnte bestemmelser i de to direktiver kan bidrage til at *fremme* »privacy by design«, har de i praksis ikke været tilstrækkelige til at *sikre*, at privatlivets fred indgår som en fast bestanddel i ikt.

36. Som følge af ovennævnte situation kræver lovgivningen ikke tilstrækkeligt præcist, at ikt udformes i overensstemmelse med »privacy by design«-princippet. Databeskyttelsesmyndighederne har heller ikke tilstrækkelige beføjelser til at sikre, at »privacy by design« integreres som en fast bestanddel. Dette resulterer i ineffektivitet. F.eks. kan databeskyttelsesmyndighederne ganske vist være i stand til at pålægge sanktioner for manglende besvarelse af anmodninger om adgang indgivet af enkeltpersoner og have kompetence til at kræve, at visse foranstaltninger gennemføres for at forhindre ulovlig behandling. Alligevel er det ikke altid tilstrækkeligt klart, om deres beføjelser også giver mulighed for at kræve, at et system udformes på

([1]) Europa-Parlamentets og Rådets direktiv 95/46/EF (i det følgende benævnt »databeskyttelsesdirektivet«).

([2]) Europa-Parlamentets og Rådets direktiv 2002/58/EF (i det følgende benævnt »e-databeskyttelsesdirektivet«).

([3]) Fortolkning af de væsentligste elementer og betingelser i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK), som blev vedtaget i Rom den 4. november 1950, da de finder anvendelse på forskellige områder.

([4]) Lissabontraktaten har styrket denne beskyttelse ved at anerkende respekten for privatliv og beskyttelse af personoplysninger som særskilte grundlæggende rettigheder i artikel 7 og 8 i EU's charter om grundlæggende rettigheder. EU's charter om grundlæggende rettigheder blev bindende, da Lissabontraktaten trådte i kraft.

([5]) Artikel 17 har følgende ordlyd: »Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling«. Dette suppleres i betragtning 46: »beskyttelsen af de registreredes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger forudsætter, at der træffes de fornødne tekniske og organisatoriske foranstaltninger både under selve udformningen og under iværksættelsen af en behandling, navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet behandling«.

([6]) Kommissionen har bekendtgjort planer om at ajourføre direktiv 1999/5/EF i slutningen af 2010.

en måde, der fremmer enkeltpersoners databeskyttelsesrettigheder ([1]). F.eks. er det på grundlag af de eksisterende lovbestemmelser uklart, om det kan kræves, at et informationssystems arkitektur udformes på en måde, der letter virksomheders besvarelse af anmodninger om adgang indgivet af enkeltpersoner, således at sådanne anmodninger kan behandles automatisk og hurtigere. Desuden kan senere forsøg på at ændre teknologien, når den er blevet udviklet eller ibrugtaget, resultere i et kludetæppe af løsninger, som ikke fungerer fuldt ud, foruden at være økonomisk bebyrdende.

37. Efter EDPS' opfattelse, som deles af Artikel 29-Gruppen ([2]), er der i lyset af den nuværende lovgivningsramme mulighed for en mere udtrykkeligt tilslutning til »privacy by design«-princippet.

IV.2. **Integrering af »privacy by design« på forskellige niveauer**

38. På baggrund af ovenstående anbefaler EDPS Kommissionen at lægge fire fremgangsmåder til grund:

a) Overveje at medtage en generel bestemmelse om »privacy by design« i lovgivningsrammen for databeskyttelse.

b) Uddybe denne generelle bestemmelse nærmere i specifikke bestemmelser, når der foreslås specifikke lovgivningsinstrumenter i forskellige sektorer. Disse specifikke bestemmelser kunne allerede nu indgå i lovgivningsinstrumenter; på grundlag af databeskyttelsesdirektivets artikel 17 (og anden eksisterende lovgivning).

c) Lade »privacy by design« indgå som et ledende princip i forbindelse med den digitale dagsorden for Europa.

d) Indføre »privacy by design« som et princip i forbindelse med andre EU-initiativer (hovedsagelig ikke-lovgivningsmæssige).

En generel bestemmelse om »privacy by design«

39. EDPS foreslår at lade »privacy by design«-princippet indgå klart og eksplicit i den eksisterende lovgivningsramme for databeskyttelse. Dette vil gøre »privacy by design«-princippet stærkere, mere eksplicit, og det vil tvinge til en effektiv gennemførelse heraf og desuden give de håndhævende myndigheder legitimitet til at kræve en faktisk anvendelse heraf i praksis. Dette er navnlig nødvendigt i lyset af ovenstående, ikke kun betydningen af selve princippet som et redskab til at fremme tillid, men også som et incitament for interessenter til at gennemføre »privacy by design« og styrke de garantier, der findes i den eksisterende lovgivningsramme.

40. Dette forslag bygger på Artikel 29-Gruppens anbefaling af at indføre »privacy by design«-princippet som et generelt princip i lovgivningsrammen for databeskyttelse, navnlig i databeskyttelsesdirektivet. Artikel 29-Gruppen har udtalt følgende: »Dette princip bør være bindende for teknologidesignere og –producenter såvel som for registeransvarlige, der skal træffe beslutning om indkøb og anvendelse af ikt. De bør være forpligtet til at indtænke teknologier til databeskyttelse allerede i planlægningsfasen af informationsteknologiske procedurer og systemer. Både leverandørerne af sådanne systemer eller –tjenester og de registeransvarlige bør vise, at de har truffet alle nødvendige foranstaltninger til at opfylde disse krav«.

41. EDPS glæder sig også over kommissær Viviane Redings støtte til »privacy by design«-princippet, da hun bekendtgjorde revisionen af databeskyttelsesdirektivet ([3]).

42. Dette fører til indholdet af en sådan regulering. For det første og som det vigtigste bør et generelt »privacy by design«-princip være teknologisk neutralt. Princippet bør ikke have til formål at regulere teknologien, dvs. det bør ikke foreskrive specifikke tekniske løsninger. I stedet bør det påbyde, at eksisterende principper for privatlivs- og databeskyttelse integreres i informations- og kommunikationssystemer og –løsninger. Dette vil gøre det muligt for

([1]) Se rapport fra UK Information Commissioner's Office med titlen »Privacy by Design«, offentliggjort i november 2008.

([2]) Se Artikel 29-Gruppen, udtalelse 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« (fremtiden for privatlivets fred, fælles bidrag til Europa-Kommissionens høring om den retlige ramme for den grundlæggende ret til beskyttelse af personoplysninger), vedtaget den 1. december 2009.

([3]) »Privacy by design« er et princip, der er i både borgernes og virksomhedernes interesse. »Privacy by design« vil føre til en bedre beskyttelse for enkeltpersoner samt til tillid og tiltro til nye tjenester og produkter, hvilket på sin side vil have en positiv indvirkning på økonomien. Der findes en række opmuntrende eksempler, men der er behov for at gøre meget mere. Hovedtale i forbindelse med databeskyttelsesdagen den 28. januar 2010, Europa-Parlamentet, Bruxelles.

interessenter, producenter, registeransvarlige og databeskyttelsesmyndigheder at fortolke betydningen af princippet i hvert enkelt tilfælde. For det andet bør det være obligatorisk at overholde princippet i forskellige faser, lige fra skabelsen af standarder og udformningen af arkitekturen til den registeransvarliges gennemførelse heraf.

Bestemmelser i specifikke lovgivningsinstrumenter

43. Nuværende og kommende lovgivningsinstrumenter skal integrere »privacy by design«-princippet på grundlag af den nuværende lovgivningsramme og efter vedtagelsen af den generelle bestemmelse, der er foreslået ovenfor, på grundlag af denne bestemmelse. F.eks. vil Kommissionen i overensstemmelse med de nuværende initiativer i forbindelse med intelligente transportsystemer have det specifikke indledende ansvar for fastlæggelsen af foranstaltninger, standardiseringsinitiativer, procedurer og bedste praksis. Ved udførelsen af disse opgaver bør »privacy by design« være det ledende princip.

44. EDPS bemærker endvidere, at »privacy by design«-princippet også er af specifik betydning i området med frihed, sikkerhed og retfærdighed, navnlig med hensyn til målene for informationsstyringsstrategien som fastsat i Stockholmprogrammet ([1]). I sin udtalelse vedrørende Stockholmprogrammet understregede EDPS, at arkitekturen for udveksling af oplysninger bør bygge på »indbygget databeskyttelse« ([2]): »Dette betyder mere konkret, at informationssystemer, der er udformet med henblik på den offentlige sikkerhed, altid bør være udviklet i overensstemmelse med principperne for »indbygget databeskyttelse««.

45. I Artikel 29-Gruppens udtalelse om fremtiden for privatlivets fred ([3]) understreges det endnu mere præcist, at krav om »privacy by design« bør gøres obligatoriske i et område med frihed, sikkerhed og retfærdighed — hvor de offentlige myndigheder er de vigtigste aktører, og hvor foranstaltninger, der øger overvågningen, indvirker direkte på de grundlæggende rettigheder til privatlivs- og databeskyttelse. Ved at indføre disse krav i informationssystemer vil de offentlige myndigheder også stimulere »privacy by design« i deres egenskab af igangsættende kunder.

»Privacy by design« som et ledende princip i forbindelse med den digitale dagsorden for Europa

46. Informations- og kommunikationsteknologier er stadig mere komplekse og forbundet med større risici for privatlivs- og databeskyttelsen. Generelt er digitaliseret information, som er lettere at få adgang til, kopiere og videregive, udsat for meget større risici end papirbaseret information. Efterhånden som vi går i retning af netværk af indbyrdes forbundne ting, vil risiciene øges. Jo større risiciene for privatlivs-/databeskyttelsen er, desto større vil efterspørgslen efter øgede foranstaltninger til data- og privatlivsbeskyttelse være. Der er derfor mere tvingende grunde til behovet for at gennemføre »privacy by design« i ikt-sektoren. Som nævnt ovenfor er enkeltpersoners tillid til ikt desuden af afgørende betydning, hvis borgerne skal tage disse nye tjenester til sig, og privatlivs- og databeskyttelse er vigtige elementer i en sådan tillid.

47. Ovenstående understreger, at en strategi for udviklingen af ikt skal bekræfte behovet for, at de udformes med et indbygget element af privatlivs- og databeskyttelse, dvs. indtænkning af »privacy by design«-princippet.

48. Den digitale dagsorden for Europa bør derfor udtrykkeligt støtte »privacy by design«-princippet som et nødvendigt element til at sikre borgernes tillid til ikt og onlinetjenester. Den bør anerkende, at privatlivets fred og tillid går hånd i hånd, og at »privacy by design« bør være en ledende faktor i udviklingen af en troværdig ikt-sektor.

»Privacy by design« som et princip i forbindelse med andre EU-initiativer

49. Kommissionen bør have »privacy by design« som et ledende princip ved gennemførelsen af politikker, aktiviteter og initiativer i specifikke ikt-sektorer, herunder e-sundhed, e-indkøb, e-social sikring, e-læring osv. Mange af disse initiativer vil være indsatspunkter i den digitale dagsorden for Europa.

50. Dette betyder f.eks., at initiativer til at sikre, at forvaltningsapplikationer er mere effektive og moderne, således at borgerne kan kommunikere med myndighederne, bør omfatte behovet for, at de udformes og gennemføres i overensstemmelse med »privacy by design«-princippet. Det samme gør sig gældende for Kommissionens politikker og aktiviteter, som vedrører hurtigere internet, digitalt indhold eller generel fremme af fast og trådløs kommunikation og datatransmission.

([1]) Stockholmprogrammet — Et åbent og sikkert Europa i borgernes tjeneste og til deres beskyttelse, vedtaget af Det Europæiske Råd i december 2009.

([2]) Udtalelse af 10. juli 2009 om meddelelsen fra Kommissionen til Europa-Parlamentet og Rådet om et område med frihed, sikkerhed og retfærdighed i borgernes tjeneste, EUT C 276, af 17.11.2009, s. 8, punkt 60.

([3]) Artikel 29-Gruppen, udtalelse 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« (fremtiden for privatlivets fred, fælles bidrag til Europa-Kommissionens høring om den retlige ramme for den grundlæggende ret til beskyttelse af personoplysninger), vedtaget den 1. december 2009.

51. Ovenstående omfatter også områder, hvor Kommissionen har ansvaret for store it-systemer, f.eks. SIS og VIS, samt de tilfælde, hvor Kommissionens ansvar kun omfatter udviklingen og vedligeholdelsen af den fælles infrastruktur for et sådant system, f.eks. det europæiske informationssystem vedrørende strafferegistre (ECRIS).

52. Hvordan »privacy by design«-princippet nøjagtigt vil blive udviklet, afhænger af den enkelte sektor og situation. F.eks. når Kommissionens initiativer er ledsaget af lovgivningsforslag vedrørende en specifik ikt-sektor, vil det i mange tilfælde være hensigtsmæssigt at tilføje en udtrykkelig henvisning til begrebet »privacy by design« i forbindelse med udformningen af ikt-applikationen/-systemet. Hvis der udformes handlingsplaner for et specifikt område, bør de systematisk sikre, at lovgivningsrammen anvendes, og mere specifikt garantere, at den relevante ikt-teknologi bygges med tanke på »privacy by design«.

53. Med hensyn til forskning bør det syvende rammeprogram og de efterfølgende programmer anvendes som et redskab til at støtte projekter, der har til formål at analysere standarder, ikt-teknologier og –arkitektur, der bedre tilgodeser privatlivets fred og især »privacy by design«-princippet. Desuden bør »privacy by design« også være et nødvendigt element, der skal tages i betragtning i bredere ikt-projekter, som tager sigte på at behandle personoplysninger.

Områder af særlig interesse

54. På grund af de særlige risici for enkeltpersoners privatlivs- og databeskyttelse eller som følge af andre faktorer (modstand i branchen mod at levere »privacy by design«-produkter, forbrugerkrav osv.) kan det i nogle tilfælde være nødvendigt at definere mere eksplicitte og specifikke »privacy by design«-foranstaltninger, som skal integreres i en given form for informations- og kommunikationsprodukt/-teknologi, hvad enten det er i lovgivningsinstrumenter eller ikke.

55. EDPS har kortlagt forskellige områder (RFID, sociale netværks- og browserapplikationer), som efter EDPS' opfattelse i denne fase bør tages op til omhyggelig overvejelse af Kommissionen, og de mere praktiske indgreb, der er anbefalet ovenfor. Disse tre områder behandles nedenfor.

V. **RADIOFREKVENSBASERET IDENTIFIKATION — RFID**

56. RFID-etiketter kan integreres i genstande, dyr og personer. De kan anvendes til at indsamle og lagre personoplysninger som f.eks. lægejournaler, følge folks bevægelser eller sammensætte deres adfærdsprofil til forskellige formål. Dette kan gøres, uden at personen er klar over det ([1]).

57. Effektive garantier for beskyttelsen af persondata og privatlivets fred og alle dertil hørende etiske forhold er af afgørende betydning for offentlighedens tillid til RFID og et fremtidigt tingenes internet. Kun i så fald kommer det store økonomiske og sociale udbytte, som teknologien kan give.

V.1. **Manglerne i den gældende lovgivningsramme for databeskyttelse**

58. Databeskyttelsesdirektivet og e–databeskyttelsesdirektivet finder anvendelse på indsamling af data via RFID-applikationer ([2]). De kræver bl.a., at der indføres tilstrækkelige foranstaltninger til privatlivsbeskyttelse for at anvende RFID-applikationer ([3]).

59. Denne lovgivningsramme afhjælper imidlertid ikke fuldt ud alle de betænkeligheder med hensyn til databeskyttelse og privatlivets fred, som denne teknologi giver anledning til. Dette skyldes, at direktiverne ikke er tilstrækkeligt detaljerede med hensyn til den form for sikkerhedsforanstaltninger, der bør indføres i forbindelse med RFID-applikationer. De eksisterende regler bør suppleres med

([1]) RFID står for radiofrekvensbaseret identifikation. Hovedbestanddelene i RFID-teknologien *eller* –infrastrukturen er en *etiket* (dvs. en mikrochip), en læser og en applikation forbundet med etiketterne og læserne via middleware og behandling af de producerede data. Etiketten består af et elektronisk kredsløb, som opbevarer data, og en antenne, hvormed dataene kan videregives via radiobølger. Læseren har en antenne og en demodulator, som oversætter de indkommende analoge oplysninger fra radioforbindelsen til digitale data. Oplysningerne kan derpå sendes via netværk til databaser og servere, således at de kan behandles af en computer.

([2]) E-databeskyttelsesdirektivet henviser til RFID i artikel 3 »Dette direktiv finder anvendelse på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr«. »Dette suppleres af betragtning 56: De teknologiske fremskridt gør det muligt at udvikle nye applikationer, som bygger på apparater til dataindsamling og identifikation, hvilket kunne være kontaktfrie apparater, der fungerer ved hjælp af radiofrekvenser. Eksempelvis benyttes der i radiofrekvensbaseret identifikation (RFID) radiofrekvenser til at opfange data fra entydigt identitetsmærkede brikker (»tags«), og disse data kan derpå overføres gennem de eksisterende kommunikationsnet. Hvis sådanne teknologier får stor udbredelse, kan de give et stort økonomisk og samfundsmæssigt udbytte og dermed yde et væsentligt bidrag til det indre marked, hvis borgerne kan acceptere, at de bruges. For at opnå dette mål er det nødvendigt at sørge for, at alle det enkelte menneskes grundlæggende rettigheder beskyttes, herunder retten til privatlivets fred og til beskyttelse af persondata. Når sådanne anordninger forbindes med offentligt tilgængelige elektroniske kommunikationsnet eller indgår som grundlæggende infrastruktur i elektroniske kommunikationstjenester, bør de relevante bestemmelser i direktiv 2002/58/EF (direktivet om databeskyttelse inden for elektronisk kommunikation), herunder bestemmelserne om sikkerhed, trafikdata og lokaliseringsdata samt om kommunikationshemmelighed, finde anvendelse.«

([3]) F.eks. er der i databeskyttelsesdirektivets artikel 17 fastsat en forpligtelse til at iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse eller ubeføjet udbredelse.

yderligere regler, som indfører specifikke sikkerhedsforanstaltninger, navnlig ved at gøre det obligatorisk at integrere tekniske løsninger (»privacy by design«) i RFID-teknologien. Dette gælder for etiketter, der lagrer personoplysninger, som bør forsynes med en »kill command«, og anvendelsen af kryptografi i etiketter, der lagrer visse typer af personoplysninger.

V.2. **Selvregulering som et første skridt**

60. I marts 2007 vedtog Kommissionen en meddelelse [1], hvoraf det bl.a. fremgik, at der var behov for at give detaljerede retningslinjer for den praktiske gennemførelse af RFID, og det var ønskeligt at vedtage konstruktionskriterier for at forebygge risici for privatlivets fred og sikkerheden.

61. For at opnå disse mål vedtog Kommissionen i maj 2009 en henstilling om gennemførelse af principperne om beskyttelse af personoplysninger og privatlivets fred i forbindelse med RFID-applikationer [2]. I RFID-applikationer i detailsektoren skal etiketterne deaktiveres ved salgsstedet, medmindre personerne har givet deres samtykke. Dette gælder, medmindre en konsekvensvurdering vedrørende privatlivs- og databeskyttelse viser, at etiketter ikke udgør en sandsynlig trussel mod privatlivets fred eller beskyttelsen af personoplysninger, i hvilket tilfælde de forbliver aktive efter salgsstedet, medmindre personerne vælger at få dem deaktiveret eller fjernet gratis.

62. EDPS er enig i Kommissionens tilgang til anvendelsen af selvregulerende instrumenter. Som nævnt nedenfor er det imidlertid tænkeligt, at selvregulering ikke vil give de forventede resultater; EDPS opfordrer derfor Kommissionen til at være parat til at vedtage alternative foranstaltninger.

V.3. **Områder, der giver anledning til betænkeligheder, og mulige yderligere foranstaltninger, hvis selvreguleringen ikke lykkes**

63. EDPS er betænkelig ved, at organisationer, der anvender RFID-applikationer i detailsektoren, kan overse muligheden for, at RFID-etiketter kan overvåges af uønskede tredjeparter. En sådan overvågning kunne afsløre personoplysninger, der (eventuelt) er lagret i etiketten, men kunne også gøre det muligt for en tredjepart at følge eller genkende en person over tid ved blot at anvende de unikke identifikatorer, der er indeholdt i en eller flere etiketter, som bæres af personen, i et miljø, der endog kan være uden for RFID-applikationens operationelle omkreds. EDPS er endvidere betænkelig ved, at operatører af RFID-applikationer kan være fristet til uretmæssigt at anvende undtagelsen og derfor lade etiketten forblive aktiv efter salgsstedet.

64. Hvis ovennævnte forekommer, kan det være for sent at mindske risiciene for enkeltpersoners databeskyttelse og privatliv, som allerede kan være blevet berørt. I betragtning af arten af selvregulering kan nationale håndhævende myndigheder desuden stå svagere, når de kræver, at organisationer, der anvender RFID-applikationer, anvender specifikke »privacy by design«-foranstaltninger.

65. I lyset af ovennævnte opfordrer EDPS Kommissionen til at være parat til at foreslå lovgivningsinstrumenter, der fastsætter regler for de vigtigste spørgsmål vedrørende brugen af RFID i tilfælde af, at den nuværende lovgivningsramme ikke gennemføres effektivt. Kommissionens vurdering bør ikke udsættes unødigt; en udsættelse vil bringe enkeltpersoner i fare og også have uheldige følger for branchen, da den retlige usikkerhed er for stor, og de rodfæstede problemer formentlig vil blive vanskeligere og dyrere af rette op på.

66. Inden for de foranstaltninger, der i givet fald bør foreslås, anbefaler EDPS anvendelse af opt-in-princippet på salgsstedet, hvorefter alle RFID-etiketter, der er knyttet til forbrugsvarer, automatisk vil blive deaktiveret på salgsstedet. Det er i givet fald ikke nødvendigt eller hensigtsmæssigt, at Kommissionen specificerer den konkrete teknologi, der skal anvendes. I stedet skal EU-retten fastsætte den retlige forpligtelse til at opnå opt-in-samtykke, hvorved operatørerne får mulighed for at afgøre, hvordan de vil opfylde kravet.

V.4. **Yderligere spørgsmål, der kan tages under overvejelse: forvaltning af tingenes internet**

67. Oplysninger, der er produceret af RFID-etiketter — f.eks. produktinformation — kan efterhånden forbindes indbyrdes til et globalt netværk af kommunikationsinfrastruktur. Dette omtales normalt som »tingenes internet«. Spørgsmålene vedrørende databeskyttelse/privatlivets fred opstår, fordi genstande fra realverdenen kan blive identificeret af RFID-etiketter, der foruden produktinformation også kan omfatte personoplysninger.

68. Der er mange åbne spørgsmål med hensyn til, hvem der vil forvalte lagringen af oplysninger i forbindelse med mærkede genstande. Hvordan vil det blive organiseret? Hvem vil havde adgang dertil? I juni 2009 vedtog Kommissionen en meddelelse om tingenes internet [3], som udtrykkeligt har kortlagt de potentielle problemer med hensyn til databeskyttelse og privatlivets fred, som dette fænomen giver anledning til.

---

[1] Meddelelse fra Kommissionen af 15.3.2007 til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme, KOM(2007) 96 endelig.

[2] Kommissionens henstilling af 12.5.2009 om gennemførelse af principperne om beskyttelse af personoplysninger og privatlivets fred i forbindelse med anvendelse af radiofrekvensbaseret identifikation (K(2009) 3200 endelig).

[3] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om tingenes internet – en EU-handlingsplan, 18.6.2009, KOM(2009) 278 endelig.

69. EDPS vil gerne understrege nogle af de spørgsmål, der er rejst i meddelelsen, og som efter EDPS' opfattelse bør behandles nærmere, efterhånden som tingenes internet udvikler sig. For det første kan behovet for en decentraliseret arkitektur fremme ansvarlighed og muligheden for at håndhæve EU-lovgivningsrammen. For det andet bør personers ret til ikke at blive sporet opretholdes i det omfang, det er muligt. Der bør med andre ord være meget få tilfælde, hvor personer spores via RFID-etiketter uden deres samtykke. Et sådant samtykke bør være eksplicit. Dette omtales normalt som »den tavse chip« og retten til at være i fred. Endelig bør »privacy by design«-princippet være et ledende princip ved udformningen af tingenes internet. F.eks. ville dette kræve, at konkrete RFID-applikationer, som har indbyggede mekanismer, der kan give brugerne kontrol, udformes med privatlivsvenlige standardindstillinger.

70. EDPS forventer at blive hørt, når Kommissionen gennemfører de aktiviteter, der er anført i meddelelsen, navnlig udarbejdelsen af meddelelsen om privatlivets fred og tilliden til det allestedsnærværende informationssamfund.

VI. SOCIALE NETVÆRK OG BEHOVET FOR PRIVATLIVSVENLIGE STANDARDINDSTILLINGER

71. Sociale netværk er »flavour of the month«. De synes at have overgået e-mail i popularitet. De forbinder folk med hinanden, som deler samme interesser og/eller aktiviteter. Folk kan have deres profiler online og dele mediefiler som f.eks. videoer, fotos, musik samt deres karriereprofiler.

72. De unge har hurtigt taget sociale netværksaktiviteter til sig, og denne tendens fortsætter. Internetbrugernes gennemsnitsalder i Europa er faldet i de seneste par år: 9-10-årige kobler sig nu op flere gange om ugen, og 12-14-årige går på internettet dagligt, ofte i 1-3 timer.

VI.1. Sociale netværk og den gældende lovgivningsramme for databeskyttelse og privatlivets fred

73. Udviklingen af sociale netværk har gjort det muligt for brugerne at uploade oplysninger om dem selv og tredjeparter på internettet. Ifølge Artikel 29-Gruppen [1] handler internetbrugerne herved som registeransvarlige, jf. databeskyttelsesdirektivets artikel 2, litra d), med hensyn til de oplysninger, som de uploader [2]. I de fleste tilfælde er en sådan behandling imidlertid omfattet af undtagelsen ved udøvelse af familiemæssige aktiviteter, jf. direktivets artikel 3, stk. 2. Samtidig betragtes sociale netværkstjenester som registeransvarlige, for så vidt som de leverer midlerne til behandling af brugerdata og yder alle de basale tjenester i forbindelse med brugerstyringen (f.eks. registrering og sletning af konti).

74. I juridisk henseende betyder dette, at internetbrugere og sociale netværkstjenester har et fælles ansvar for behandlingen af personoplysninger som »registeransvarlige« som omhandlet i direktivets artikel 2, litra d), omend i forskelligt omfang og med forskellige forpligtelser.

75. Brugerne bør derfor vide og forstå, at de ved at behandle egne og andres personoplysninger er omfattet af EU-lovgivningens bestemmelser om databeskyttelse, som bl.a. kræver informeret samtykke fra de personer, hvis oplysninger uploades, og at de pågældende gives ret til berigtigelse, indsigelsesret osv. Ligeledes skal sociale netværkstjenester bl.a. iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at forhindre ulovlig behandling, i forhold til de risici, som behandlingen indebærer, og oplysningernes art. Dette betyder igen, at sociale netværkstjenester bør sikre privatlivsvenlige standardindstillinger, herunder indstillinger, der begrænser profiladgangen til kontakter, som brugeren selv har valgt. Indstillinger bør også kræve brugerens udtrykkelige samtykke, inden en profil bliver tilgængelig for andre tredjeparter, og begrænsede adgangsprofiler skal ikke kunne registreres af interne søgemaskiner.

76. Der er desværre en kløft mellem lovgivningskravene og den faktiske overholdelse. Mens internetbrugere juridisk set betragtes som registeransvarlige og er bundet af EU's lovgivningsramme for databeskyttelse og privatlivets fred, er de i realiteten ofte ikke klar over denne rolle. Generelt har de en ringe forståelse for, at de behandler personoplysninger, og at offentliggørelsen af sådanne oplysninger er forbundet med risici for privatlivs- og databeskyttelsen. Navnlig unge lægger indhold ud på internettet og undervurderer konsekvenserne for sig selv og andre, f.eks. i forbindelse med en senere optagelse på uddannelsesinstitutioner eller jobansøgninger.

[1] Se Artikel 29-Gruppen, 163, udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter, vedtaget den 12. juni 2009.

[2] »Den registeransvarlige«: den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller i fællesskabsretten.

77. Samtidig vælger udbydere af sociale netværkstjenester ofte på forhånd standardindstillinger, der er baseret på »opt-out«-klausuler, så det gøres lettere at videregive personoplysninger. Nogle giver mulighed for, at profiler er tilgængelige for almindelige søgemaskiner som standard. Dette rejser spørgsmål med hensyn til, om enkeltpersoner faktisk har givet deres samtykke til videregivelse, samt om sociale netværk har overholdt direktivets artikel 17 (beskrevet ovenfor), hvorefter de skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at forhindre ulovlig behandling.

VI.2. **Risici ved sociale netværk og foreslåede foranstaltninger til at mindske dem**

78. Ovenstående resulterer i et øget risiko for personers privatlivs- og databeskyttelse. Det udsætter internetbrugere og personer, hvis oplysninger er blevet uploadet, for åbenlyse krænkelser af deres privatlivs- og databeskyttelse.

79. På denne baggrund er det spørgsmål, som Kommissionen bør tage fat på, hvad der bør og kan gøres for at rette op på denne situation. Denne udtalelse giver ikke et fuldstændigt svar på spørgsmålet, men indeholder i stedet en række forslag til nærmere overvejelse.

Investering i uddannelse af internetbrugere

80. Det første forslag er at investere i brugeruddannelse. I denne henseende bør EU-institutionerne og de nationale myndigheder investere i uddannelse og øge bevidstheden om truslerne fra sociale netværkssites. Generaldirektoratet for Informationssamfundet har f.eks. gennemført Safer Internet-programmet, der har til formål at hjælpe og beskytte børn og unge gennem f.eks. oplysningsaktiviteter ([1]). For nylig lancerede EU-institutionerne kampagnen »Tænk før du uploader« for at øge bevidstheden om risiciene ved at dele personoplysninger med fremmede.

81. EDPS opfordrer Kommissionen til fortsat at støtte denne form for aktivitet. Udbyderne af sociale netværk bør imidlertid selv også spille en aktiv rolle, da de har et juridisk og socialt ansvar for at uddanne brugerne i, hvordan deres tjenester bruges på en sikker og brugervenlig måde.

82. Som nævnt ovenfor kan de oplysninger, der lægges ud på sociale netværk, i givet fald som standard gøres tilgængelige på en række forskellige måder. F.eks. kan oplysningerne være tilgængelige for offentligheden generelt, herunder søgemaskiner, som kan indeksere dem og derved etablere direkte links til dem. På den anden side kan oplysningerne være begrænset til »udvalgte venner« eller holdes fuldstændig privat. Profiltilladelserne og den anvendte terminologi varierer tydeligvis fra websted til websted.

83. Det er som anført ovenfor imidlertid kun meget få brugere af sociale netværkstjenester, der ved, hvordan de kan kontrollere adgangen til de oplysninger, de lægger ud, eller hvordan de ændrer de privatlivsindstillinger, der er valgt som standard. Privatlivsindstillinger forbliver normalt uændrede, da brugerne ikke er klar over følgerne af ikke at ændre dem eller ikke ved, hvordan det gøres. Den omstændighed, at personer ikke ændrer privatindstillingerne, betyder derfor som oftest ikke, at de har truffet en informeret beslutning om at acceptere at dele oplysninger. I denne forbindelse er det navnlig vigtigt, at tredjeparter som f.eks. søgemaskiner ikke linker til individuelle profiler ud fra den antagelse, at brugerne som standard (ved ikke at ændre privatlivsindstillingerne) har givet samtykke til at gøre oplysningerne tilgængelige uden begrænsninger.

84. Selv om brugeruddannelse kan bidrage til at rette op på denne situation, vil dette ikke være tilstrækkeligt. Som anbefalet af Artikel 29-Gruppen i dens udtalelse om sociale netværk bør udbydere af sociale netværk tilbyde privatlivsvenlige standardindstillinger gratis. Dette vil gøre brugerne mere bevidste om deres handlinger og sætte dem i stand til at foretage bedre valg med hensyn til, om de ønsker at dele oplysninger og med hvem.

Selvregulering kan spille en rolle

85. Kommissionen har indgået en aftale med 20 udbydere af sociale netværk kaldet »Safer Social Networking Principles for the EU« ([2]). Formålet med aftalen er at forbedre mindreåriges sikkerhed, når de bruger sociale netværkssites i Europa. Sådanne principper omfatter mange af de krav, der er afledt af anvendelsen af den lovgivningsramme for databeskyttelse, der er beskrevet ovenfor. De omfatter f.eks. kravet om at forsyne brugerne med redskaber og teknologi for at sikre, at de kan kontrollere anvendelsen og formidlingen af deres personoplysninger. Det omfatter også behovet for at sørge for privatlivsvenlige standardindstillinger.

86. I begyndelsen af januar 2010 offentliggjorde Kommissionen resultaterne i en rapport med evaluering af gennemførelsen af principperne ([3]). EDPS er betænkelig ved, at det fremgår af denne rapport, at selv om nogle foranstaltninger er blevet truffet, er det ikke tilfældet med hensyn til mange andre. F.eks. var der ifølge rapporten

([1]) Oplysninger om dette program findes på: http://ec.europa.eu/information_society/activities/sip/index_en.htm

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

([3]) »Report on the assessment of the implementation of the Safer Social Network Principles for the EU« (rapport om vurderingen af gennemførelsen af principperne for sikrere sociale netværk for EU), findes på: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

problemer med hensyn til kommunikationen af de sikkerhedsforanstaltninger og –redskaber, der er tilgængelige på webstederne. Det fremgik endvidere, at under halvdelen af dem, der har undertegnet aftalen, kun begrænser adgangen til mindreåriges profiler til deres venner.

Behov for obligatoriske privatlivsvenlige standardindstillinger

87. I denne forbindelse er det vigtige spørgsmål, om der er behov for yderligere politiktiltag for at sikre, at sociale netværk opretter deres tjenester med privatlivsvenlige standardindstillinger. Dette spørgsmål blev rejst af den tidligere kommissær for informationssamfundet, Viviane Reding, som pegede på, at lovgivning kan være nødvendig ([1]). I samme retning anførte Det Europæiske Økonomiske og Sociale Udvalg, at der ved siden af selvregulering bør indføres mindstebeskyttelsesstandarder ved lov ([2]).

88. Som bemærket ovenfor kan forpligtelsen for udbydere af sociale netværk til at indføre privatlivsvenlige standardindstillinger udledes indirekte af databeskyttelsesdirektivets artikel 17 ([3]), som forpligter registeransvarlige til at iværksætte de fornødne tekniske og organisatoriske foranstaltninger (»både under selve udformningen og under iværksættelsen af en behandling«) for at varetage sikkerheden og forhindre ulovlig behandling, i forhold til de risici, som behandlingen indebærer, og oplysningernes art.

89. Denne artikel er imidlertid alt for generel og mangler specificitet, også i denne forbindelse. Det anføres ikke klart, hvad der menes med de fornødne tekniske og organisatoriske foranstaltninger i forbindelse med sociale netværk. Den nuværende situation er derfor præget af retlig usikkerhed, der forårsager problemer for både lovgivere og enkeltpersoner, hvis privatliv og personoplysninger ikke er fuldt ud beskyttet.

90. På baggrund af ovenstående opfordrer EDPS Kommissionen til at udarbejde lovgivning, der som et minimum indeholder en overordnet forpligtelse, som kræver obligatoriske privatlivsindstillinger, sammen med mere præcise krav:

a) Sørge for indstillinger, der begrænser adgangen til brugerprofiler til kontakter, som brugeren selv har valgt. Indstillingerne bør også kræve brugerens udtrykkelige samtykke, inden en profil er tilgængelig for tredjeparter.

b) Sørge for, at begrænsede adgangsprofiler ikke kan registreres af interne/eksterne søgemaskiner.

91. Ud over at sørge for obligatoriske privatlivsvenlige standardindstillinger er det fortsat et spørgsmål, om yderligere specifikke databeskyttelsesforanstaltninger og andre foranstaltninger (f.eks. vedrørende beskyttelse af mindreårige) også kan være hensigtsmæssige. Dette rejser det bredere spørgsmål, om det vil være hensigtsmæssigt at etablere en specifik ramme for denne form for tjenester, som foruden at sørge for obligatoriske privatlivsindstillinger vil regulere andre aspekter. EDPS anmoder Kommissionen om at tage dette spørgsmål under overvejelse.

VII. **PRIVATLIVSVENLIGE STANDARDBROWSERINDSTILLINGER FOR AT GARANTERE INFORMERET SAMTYKKE TIL AT MODTAGE ANNONCER**

92. Udbydere af annoncenetværk anvender cookies og andet udstyr til at overvåge individuelle brugeres adfærd, når de surfer på internettet, for at katalogisere deres interesser og opbygge profiler. Disse oplysninger anvendes derpå til at sende dem målrettede annoncer ([4]).

VII.1. **Tilbageværende udfordringer og risici i forbindelse med den nuværende lovgivningsramme for databeskyttelse/privatlivets fred**

93. Denne behandling er omfattet af databeskyttelsesdirektivet (hvad angår personoplysninger) og også af e-databeskyttelsesdirektivets artikel 5, stk. 3. I denne artikel kræves det specifikt, at brugeren informeres og gives mulighed for at reagere ved at give sit samtykke til eller nægte, at f.eks. cookies lagres på brugerens computer eller anden enhed ([5]).

94. Hidtil har udbydere af annoncenetværk anvendt browserindstillinger og privatlivspolitikker til at informere brugerne og give dem mulighed for at give deres samtykke til eller nægte cookies. De har forklaret i forbindelse med udgiverens privatlivspolitik, hvordan man kan

([1]) Viviane Reding, medlem af Europa-Kommissionen med ansvar for informationssamfundet og medier. »Think before you post! How to make social networking sites safer for children and teenagers?« (Tænk før du uploader! Hvordan gøres sociale netværkssites mere sikre for børn og teenagere?), Sikker Internet Dag Strasbourg, 9. februar 2010.

([2]) Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om »The Impact of social network sites on citizens/consumers« (sociale netværkssites' indvirkning på borgere/forbrugere), 4. november 2009.

([3]) Også behandlet i punkt 33 i dette dokument.

([4]) Sporingscookies er små tekstfiler, der indeholder en unik identifikator. Typisk placerer udbydere af annoncenetværk (såvel som webstedsoperatører eller -udgivere) cookies på de besøgendes harddisk, navnlig i internetbrugeres browser, når brugerne første gang besøger annonceunderstøttede websteder, der indgår i deres netværk. Cookien vil gøre det muligt for udbyderen af annoncenetværket at genkende en tidligere besøgende, som vender tilbage til det pågældende websted, eller besøger ethvert websted, der er partner i annoncenetværket. Sådanne gentagne besøg vil gøre det muligt for udbyderen af annoncenetværket at opbygge en profil af den besøgende.

([5]) E-databeskyttelsesdirektivets artikel 5, stk. 3, blev for nylig ændret for at styrke beskyttelsen mod opsnapning af brugerkommunikation ved hjælp af — f.eks. — spyware og cookies, der er lagret på en brugers computer eller anden enhed. I det nye direktiv bør brugerne tilbydes bedre oplysninger og lettere måder til at kontrollere, om de ønsker cookies lagret i deres terminaludstyr.

fravælge i det hele taget at modtage cookies eller acceptere dem i hvert enkelt tilfælde. Hensigten hermed var at overholde deres forpligtelse til at tilbyde brugerne ret til at nægte cookies.

95. Mens denne metode (via browseren) i teorien virkelig effektivt kunne tilvejebringe et meningsfuldt informeret samtykke, er realiteten helt anderledes. Generelt mangler brugerne den grundlæggende forståelse af indsamlingen af alle oplysninger, endsige fra tredjeparter, af værdien af sådanne oplysninger, anvendelserne heraf, hvordan teknologien fungerer, og især, hvordan og hvor der kan foretages fravalg (opt-out). De skridt, som brugere skal tage for at foretage fravalg, synes ikke kun komplicerede, men også meget vidtgående (først skal brugeren indstille browseren til at acceptere cookies og derpå benytte opt-out-muligheden).

96. Som følge heraf benytter meget få personer i praksis opt-out-muligheden, ikke fordi de har truffet en informeret beslutning om at acceptere adfærdsbaserede annoncer, men snarere fordi de ikke erkender, at de ved ikke at benytte opt-out-muligheden faktisk accepterer det.

97. Selv om e-databeskyttelsesdirektivets artikel 5, stk. 3, juridisk set giver en effektiv retlig beskyttelse, anses internetbrugere derfor i praksis for at give samtykke til at blive overvåget med henblik på at sende adfærdsbaserede annoncer, når de faktisk i mange tilfælde — hvis ikke i de fleste tilfælde — slet ikke er klar over, at overvågningen finder sted.

98. Artikel 29-Gruppen er ved at udarbejde en udtalelse, som tager sigte på at præcisere, hvilke lovgivningskrav der gælder for adfærdsbaseret annoncering, hvilket hilses velkommen. En fortolkning er imidlertid i givet fald ikke i sig selv tilstrækkelig til at løse denne situation, og det kan være nødvendigt, at Den Europæiske Union iværksætter yderligere tiltag.

VII.2. **Behov for yderligere tiltag, navnlig med hensyn til obligatoriske privatlivsvenlige standardindstillinger**

99. Som nævnt ovenfor tillader webbrowsere sædvanligvis i et vist omfang kontrol med visse former for cookies. På nuværende tidspunkt accepterer de fleste webbrowseres standardindstillinger alle cookies. Browserne er med andre ord som standard indstillet til at acceptere alle cookies, uanset formålet med cookien. Kun hvis brugeren ændrer indstillingerne for sin browserapplikation til at nægte cookies, hvilket som nævnt meget få brugere gør, vil brugeren ikke modtage cookies. Desuden er der ingen privatlivsguide (privacy wizard) i forbindelse med den første installation eller opdatering af browserapplikationer.

100. En måde til at afhjælpe ovennævnte problem vil være, hvis browsere fik privatlivsvenlige standardindstillinger. Med andre ord hvis de fik indstillingen »ingen accept af tredjepartscookies«. Som supplement hertil og for at gøre det mere effektivt bør browserne kræve, at brugerne gennemgår en privatlivsguide, når de første gang installerer eller opdaterer browseren. Der er behov for mere granularitet og klare oplysninger om typerne af cookies og anvendeligheden af nogle af dem. Brugere, der er rede til at blive overvåget med henblik på at modtage annoncer, vil blive behørigt informeret herom, og de vil skulle ændre browserindstillingerne. Dette vil give dem en øget kontrol med deres personoplysninger og privatlivets fred. Dette vil efter EDPS' opfattelse være en effektiv måde til at respektere og opretholde brugernes samtykke [1].

101. Under hensyntagen til på den ene side problemets omfattende karakter, med andre ord antallet af internetbrugere, som på nuværende tidspunkt overvåges på grundlag af et samtykke, der er illusorisk, og på den anden side omfanget af de interesser, der er på spil, bliver behovet for yderligere sikkerhedsforanstaltninger mere akut. Gennemførelsen af »privacy by design«-princippet i webbrowserapplikationer kunne gøre en markant forskel med hensyn til at give personer kontrol med den dataindsamlingspraksis, der anvendes til annonceformål.

102. Af disse grunde opfordrer EDPS Kommissionen til at overveje lovgivningsforanstaltninger, som kræver obligatoriske privatlivsvenlige standardindstillinger i browsere og tilvejebringelse af den relevante information.

VIII. **ANDRE PRINCIPPER, SOM HAR TIL FORMÅL AT BESKYTTE PERSONERS PRIVATLIV/DATABESKYTTELSE**

103. Selv om »privacy by design«-princippet har et stort potentiale til at forbedre beskyttelsen af personoplysninger og privatlivets fred, er det nødvendigt, at der i lovgivningen udformes og gennemføres supplerende principper for at sikre forbrugernes tillid til ikt. På denne baggrund behandler EDPS ansvarlighedsprincippet og færdiggørelsen af en obligatorisk ramme for sikkerhedsbrud, som finder anvendelse på tværs af sektorer.

VIII.1. **Ansvarlighedsprincippet for at sikre overholdelse af »privacy by design«-princippet**

104. I Artikel 29-Gruppens dokument med titlen »Future of Privacy« [2] anbefaledes det at medtage ansvarlighedsprincippet i databeskyttelsesdirektivet. Ifølge dette princip,

[1] EDPS er samtidig klar over, at dette ikke vil løse problemet fuldstændigt, for så vidt som der er cookies, som ikke kan kontrolleres via browseren, f.eks. de såkaldte flash cookies. Med henblik herpå vil det være nødvendigt, at browserudviklere integrerer en flashkontrol i deres cookiekontrol som standard ved udgivelsen af nye browsere.

[2] Artikel 29-Gruppen, udtalelse 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« (fremtiden for privatlivets fred, fælles bidrag til Europa-Kommissionens høring om den retlige ramme for den grundlæggende ret til beskyttelse af personoplysninger), vedtaget den 1. december 2009.

som er anerkendt i nogle multinationale databeskyttelsesinstrumenter ([1]), skal organisationer iværksætte processer til at overholde eksisterende bestemmelser og etablere metoder til at vurdere og dokumentere overholdelse af lovgivningen og andre bindende instrumenter.

105. EDPS støtter fuldt ud Artikel 29-Gruppens anbefaling og er af den opfattelse, at dette princip vil være yderst relevant med henblik på at fremme en effektiv anvendelse af databeskyttelsesprincipper og –forpligtelser. Ansvarlighedsprincippet vil kræve, at registeransvarlige dokumenterer, at de har indført den mekanisme, der er nødvendigt for at overholde den gældende databeskyttelseslovgivning. Dette vil sandsynligvis bidrage til en effektiv gennemførelse af »privacy by design« i ikt-teknologier som et særligt velegnet instrument til at vise ansvarlighed.

106. Til at måle og dokumentere ansvarligheden kunne de registeransvarlige anvende interne procedurer og eksterne audits eller andre former for kontrol, der kan udmønte sig i mærkninger. I denne forbindelse opfordrer EDPS Kommissionen til at overveje, om det foruden et generelt ansvarlighedsprincip i givet fald er hensigtsmæssigt ved lov at kræve specifikke ansvarlighedsforanstaltninger som f.eks. behovet for at udføre konsekvensvurderinger vedrørende privatlivs- og databeskyttelse og under hvilke omstændigheder.

VIII.2. **Sikkerhedsbrud: færdiggørelse af lovgivningsrammen**

107. Ændringerne sidste år af e-databeskyttelsesdirektivet omfattede et krav om underretning af de berørte enkeltpersoner og også de relevante myndigheder om brud på datasikkerheden. Et brud på datasikkerheden defineres bredt som ethvert brud, der fører til tilintetgørelse, tab, videregivelse osv. af persondata, der sendes, lagres eller på anden måde behandles i forbindelse med tjenesten. Enkeltpersoner skal underrettes, når bruddet på datasikkerheden kan forventes at krænke deres personoplysninger eller privatlivets fred. Dette kan være tilfældet, hvis bruddet kan indebære identitetstyveri, betydelig tort eller skade af omdømme. De relevante myndigheder skal underrettes om ethvert brud på datasikkerheden, uanset om det udgør en risiko for personer.

Anvendelse af forpligtelser med hensyn til sikkerhedsbrud på tværs af sektorer

108. Desværre gælder denne forpligtelse kun for udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, f.eks. telefonselskaber, udbydere af internetadgang, webmailudbydere osv. EDPS opfordrer Kommissionen til at fremlægge forslag om sikkerhedsbrud, der gælder på tværs af sektorer. Med hensyn til indholdet af en sådan ramme mener EDPS, at lovgivningsrammen for sikkerhedsbrud i e-databeskyttelsesdirektivet sikrer en passende balance mellem beskyttelsen af personers rettigheder, herunder deres ret til beskyttelse af personoplysninger og privatlivets fred, og forpligtelserne for omfattede enheder. Samtidig er dette en ramme med effektive foranstaltninger, da den er understøttet af relevante håndhævelsesbestemmelser, som giver myndighederne tilstrækkelige undersøgelses- og sanktionsbeføjelser i tilfælde af manglende overholdelse.

109. EDPS opfordrer derfor Kommissionen til at vedtage et lovgivningsforslag, hvor denne ramme finder anvendelse på tværs af sektorer, om nødvendigt med de relevante justeringer. Dette vil desuden sikre, at de samme standarder og procedurer anvendes på tværs af sektorer.

Færdiggørelse af lovgivningsrammen i e-databeskyttelsesdirektivet efter komitologiproceduren

110. Det reviderede e-databeskyttelsesdirektiv giver Kommissionen beføjelse til at vedtage tekniske gennemførelsesforanstaltninger, dvs. detaljerede foranstaltninger vedrørende underretning om sikkerhedsbrud, efter en komitologiprocedure ([2]). Denne beføjelse er berettiget med henblik på at sikre en ensartet gennemførelse og anvendelse af lovgivningsrammen for sikkerhedsbrud. En ensartet gennemførelse bidrager til at sikre, at personer i hele Fællesskabet opnår det samme høje beskyttelsesniveau, og at omfattede enheder ikke pålægges divergerende underretningskrav.

111. E-databeskyttelsesdirektivet blev vedtaget i november 2009. Der synes ikke at være nogen begrundelse for at udsætte påbegyndelsen af arbejdet med at vedtage tekniske gennemførelsesforanstaltninger. EDPS tilrettelagde to seminarer, som havde til formål at dele og indsamle erfaringer om underretning af brud på datasikkerheden. EDPS vil gerne dele resultaterne heraf og ser frem til at arbejde sammen med Kommissionen og andre interessenter om at finjustere den generelle lovgivningsramme for brud på datasikkerheden.

112. EDPS opfordrer Kommissionen til inden for kort tid at træffe de nødvendige foranstaltninger. Inden Kommissionen vedtager tekniske gennemførelsesforanstaltninger, skal den iværksætte en bred høring, hvor ENISA, EDPS og Artikel 29-Gruppen skal høres. Endvidere skal høringen også omfatte andre »relevante aktører«, særlig med henblik på at blive informeret om de bedste tilgængelige tekniske og økonomiske midler til gennemførelsen.

([1]) OECD's retningslinjer af 1980 for beskyttelse af privatlivets fred og grænseoverskridende overførsel af personoplysninger; Madrid Privacy Declaration on Global Privacy Standards for a Global World (Madrid-erklæring om globale standarder for privatlivets fred for en global verden), af 3. november 2009.

([2]) Som led i komitologiproceduren vedtages tekniske gennemførelsesforanstaltninger via et udvalg bestående af medlemsstaternes repræsentanter under Kommissions ledelse. Med hensyn til e-databeskyttelsesdirektivet finder den såkaldte forskriftsprocedure med kontrol anvendelse, hvilket betyder, at Europa-Parlamentet og Rådet kan gøre indsigelse mod foranstaltninger, der er foreslået af Kommissionen. Se endvidere http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **KONKLUSIONER**

113. Tillid, eller snarere mangel herpå, er blevet kortlagt som et centralt spørgsmål i forbindelse med fremkomsten og den vellykkede ibrugtagning af informations- og kommunikationsteknologier. Hvis folk ikke har tillid til ikt, vil disse teknologier sandsynligvis ikke få succes. Tillid til ikt afhænger af forskellige faktorer, hvor sikringen af, at disse teknologier ikke underminerer personers grundlæggende rettigheder til privatlivets fred og beskyttelsen af personoplysninger, er en væsentlig faktor.

114. For yderligere at styrke lovgivningsrammen for databeskyttelse/privatlivets fred, hvis principper fortsat er fuldt ud relevante i informationssamfundet, foreslår EDPS, at Kommissionen integrerer »privacy by design« på forskellige niveauer i lovgivningen og den politiske beslutningsproces.

115. EDPS anbefaler Kommissionen at lægge fire fremgangsmåder til grund:

a) Overveje at medtage en generel bestemmelse om »privacy by design« i lovgivningsrammen for databeskyttelse. Denne bestemmelse bør være teknologisk neutral, og overholdelse bør være obligatorisk i forskellige faser.

b) Uddybe denne generelle bestemmelse nærmere i specifikke bestemmelser, når der foreslås specifikke lovgivningsinstrumenter i forskellige sektorer. Disse specifikke bestemmelser kunne allerede nu indgå i lovgivningsinstrumenter; på grundlag af databeskyttelsesdirektivets artikel 17 (og anden eksisterende lovgivning).

c) Lade »privacy by design« indgå som et ledende princip i den digitale dagsorden for Europa.

d) Indføre »privacy by design« som et princip i forbindelse med andre EU-initiativer (hovedsagelig ikke-lovgivningsmæssige).

116. På tre særlige ikt-områder anbefaler EDPS, at Kommissionen vurderer behovet for at fremlægge forslag til gennemførelse af »privacy by design«-princippet på specifikke måder:

a) Med hensyn til RFID at foreslå lovgivningsinstrumenter, der fastsætter regler for de vigtigste spørgsmål vedrørende brugen af RFID i tilfælde af, at den nuværende lovgivningsramme ikke gennemføres effektivt via selvregulering. Navnlig at anvende opt-in-princippet på salgsstedet, hvorefter alle RFID-etiketter, der er knyttet til forbrugsvarer, automatisk vil blive deaktiveret på salgsstedet.

b) Med hensyn til sociale netværk at udarbejde lovgivning, der som et minimum indeholder en overordnet forpligtelse, som kræver obligatoriske privatlivsindstillinger, sammen med mere præcise krav med hensyn til at begrænse adgangen til brugerprofiler til kontakter, som brugeren selv har valgt, og sørge for, at begrænsede adgangsprofiler ikke kan registreres af interne/eksterne søgemaskiner.

c) Med hensyn til målrettet annoncering at overveje lovkrav om, at browserindstillinger som standard skal nægte tredjepartscookies og kræve, at brugerne gennemgår en privatlivsguide, når de første gang installerer eller opdaterer browseren.

117. Endelig forslår EDPS Kommissionen at:

a) overveje at gennemføre ansvarlighedsprincippet i det eksisterende databeskyttelsesdirektiv og

b) udarbejde en række regler og procedurer med henblik på at gennemføre bestemmelserne om underretning om sikkerhedsbrud i e-databeskyttelsesdirektivet og udvide dem til generelt at gælde for alle registeransvarlige.

Udfærdiget i Bruxelles, den 18. marts 2010.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse