ISSN 1725-2393

Den Europæiske Unions Tidende

C 128

Dansk udgave

52. årgang

6. juni 2009

Meddelelser og oplysninger

Informationsnummer | Indhold | Side

DA

(Fortsættes på omslagets anden side)

IV *Oplysninger*

OPLYSNINGER FRA DEN EUROPÆISKE UNIONS INSTITUTIONER OG ORGANER

Kommissionen

Berigtigelser

DA

I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om den endelige rapport fra EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger

(2009/C 128/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser 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,

som henviser 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, særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING — UDTALELSENS KONTEKST

1. Den 28. maj 2008 underrettede formandskabet for Rådet for Den Europæiske Union Coreper med henblik på EU-topmødet den 12. juni 2008 om, at EU-USA-Kontaktgruppen på Højt Plan om Informationsdeling og Beskyttelse af Privatlivets Fred og Personoplysninger (i det følgende benævnt kontaktgruppen på højt plan) havde afsluttet sin rapport. Denne rapport blev offentliggjort den 26. juni 2008 ([1]).

2. Rapporten tilstræber at udpege fælles principper for beskyttelse af privatlivets fred og databeskyttelse som første skridt hen imod udveksling af oplysninger med USA for at bekæmpe terrorisme og grov grænseoverskridende kriminalitet.

3. I sin meddelelse sagde formandskabet for Rådet, at det ville hilse alle idéer med hensyn til opfølgning af denne rapport velkommen, navnlig reaktioner på de henstillinger om vejen frem, der findes i rapporten. Den tilsynsførende imødekommer denne opfordring ved at udarbejde følgende udtalelse, der bygger på den offentliggjorte status over situationen, og som ikke foregriber en eventuel senere holdning, han måtte indtage i betragtning af udviklingen i sagen.

4. Den tilsynsførende noterer sig, at arbejdet i kontaktgruppen på højt plan har fundet sted i en kontekst, der navnlig siden 11. september 2001 har været præget af udviklingen i dataudveksling mellem USA og EU gennem internationale aftaler eller andre typer instrumenter. Blandt dem er Europols og Eurojusts aftaler med USA og PNR-aftalerne og SWIFT-sagen, der førte til en udveksling af skrivelser mellem tjenestemænd i EU og USA for at fastsætte minimumsdatabeskyttelsesgarantier ([2]).

([1]) Rådsdokument nr. 9831/08 tilgængeligt på: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Aftale mellem Amerikas Forenede Stater og Den Europæiske Politienhed af 6. december 2001 og tillægsaftale mellem Europol og USA om udveksling af personoplysninger og hermed forbundne oplysninger, der er offentliggjort på Europols hjemmeside
— Aftale mellem Amerikas Forenede Stater og Eurojust om retligt samarbejde, 6. november 2006, der er offentliggjort på Eurojusts hjemmeside
— Aftale mellem Den Europæiske Union og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger til United States Department of Homeland Security (DHS) (PNR-aftale 2007) undertegnet i Bruxelles den 23. juli 2007 og i Washington den 26. juli 2007, EUT L 204 af 4.8.2007, s. 18.
— Udveksling af skrivelser mellem USA's og EU's myndigheder om programmet til sporing af finansiering af terrorisme, 28. juni 2007.

5. EU forhandler og tilslutter sig desuden lignende instrumenter om udveksling af personoplysninger med andre tredjelande. Et nyligt eksempel er aftalen mellem Den Europæiske Union og Australien om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger med oprindelse i Den Europæiske Union til det australske toldvæsen ([3]).

6. Det fremgår af denne sammenhæng, at antallet af anmodninger fra tredjelandes retshåndhævende myndigheder om personoplysninger bliver stadig større, og at den rækker fra traditionelle statslige databaser til andre typer filer, navnlig datafiler indsamlet af den private sektor.

7. Som et vigtigt baggrundselement minder den tilsynsførende også om, at spørgsmålet om videregivelse af personoplysninger til tredjelande inden for rammerne af politisamarbejde og retligt samarbejde i kriminalsager omhandles i Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager ([4]), der forventes vedtaget inden udgangen af 2008.

8. Denne transatlantiske udveksling af oplysninger kan kun forventes at vokse og berøre flere sektorer, hvor der behandles personoplysninger. I en sådan sammenhæng er en dialog om »transatlantisk retshåndhævelse« på samme tid velkommen og følsom. Den er velkommen i den forstand, at den kan give en klarere ramme for de udvekslinger af oplysninger, der finder sted eller vil finde sted. Den er også følsom, fordi en sådan ramme kan legitimere massive dataoverførsler på et område — retshåndhævelse — hvor virkningerne for de enkelte borgere er særlig alvorlige, og hvor der derfor er endnu mere behov for strenge og pålidelige sikkerhedsforanstaltninger og garantier ([5]).

9. Denne udtalelse vil i kapitel II omhandle den nuværende situation og mulige veje frem. Kapitel III vil fokusere på anvendelsesområdet for og arten af et instrument, der giver mulighed for informationsdeling. I kapitel IV vil udtalelsen generelt analysere juridiske spørgsmål i forbindelse med indholdet af en mulig aftale. Den vil tage spørgsmål op som betingelserne for vurdering af beskyttelsesniveauet i USA og drøfte spørgsmålet om anvendelsen af EU's regelsæt som et benchmark til at vurdere dette beskyttelsesniveau. Dette kapitel vil også anføre de grundlæggende krav, der skal indgå i en sådan aftale. Endelig vil udtalelsen i kapitel V indeholde en analyse af de principper til beskyttelse af privatlivets fred, der er knyttet til rapporten.

([3]) EUT L 213 af 8.8.2008, s. 49.

([4]) Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, udgave af 24. juni 2008 tilgængelig på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Med hensyn til nødvendigheden af en klar retlig ramme, jf. kapitel III og IV i denne udtalelse.

II. DEN NUVÆRENDE SITUATION OG MULIGE VEJE FREM

10. Den tilsynsførende vurderer den nuværende situation som følger. Der er gjort nogle fremskridt med hensyn til definitionen af fælles standarder for informationsdeling og beskyttelse af privatlivets fred og personoplysninger.

11. Det forberedende arbejde for en aftale mellem EU og USA er dog endnu ikke afsluttet. Der skal gøres en yderligere insats. Rapporten fra kontaktgruppen på højt plan nævner en række udestående spørgsmål, hvoraf »klagemuligheder« er det vigtigste. Der er uenighed om domstolsprøvelsens nødvendige omfang ([6]). Der er udpeget fem andre udestående spørgsmål i kapitel 3 i rapporten. Det fremgår endvidere af denne udtalelse, at der er mange andre spørgsmål, der endnu ikke er løst, f.eks. om anvendelsesområdet for og arten af et instrument for informationsdeling.

12. Eftersom rapportens foretrukne mulighed er en bindende aftale — som den tilsynsførende også foretrækker — er der desto mere behov for forsigtighed. Yderligere omhyggelige og tilbundsgående forberedelser er nødvendige, før der kan opnås enighed.

13. Endelig indgås en aftale efter den tilsynsførendes mening bedst under Lissabontraktaten, naturligvis afhængig af dens ikrafttræden. Under Lissabontraktaten vil der ikke opstå nogen juridisk uklarhed om skillelinjen mellem EU's søjler. Der vil endvidere være garanteret fuld inddragelse af Europa-Parlamentet samt judiciel kontrol ved Domstolen.

14. Under disse omstændigheder vil den bedste vej frem være at udarbejde en køreplan hen imod en mulig aftale på et senere stadium. En sådan køreplan kan indeholde følgende:

— Vejledning for det videre arbejde i kontaktgruppen på højt plan (eller enhver anden gruppe) samt en tidslinje.

— På et tidligt tidspunkt drøftelse og eventuel enighed om grundlæggende spørgsmål som aftalens anvendelsesområde og art.

— På basis af en fælles forståelse af disse grundlæggende spørgsmål videre udarbejdelse af principperne for databeskyttelse.

— Inddragelse af interessenter på forskellige stadier af proceduren.

— Fra europæisk side skal der arbejdes med de institutionelle restriktioner.

([6]) Side 5 i rapporten, under C.

III. **ANVENDELSESOMRÅDE FOR OG ART AF ET INSTRUMENT FOR INFORMATIONSDELING**

15. Det er efter den tilsynsførendes mening afgørende, at anvendelsesområdet for og arten af et eventuelt instrument, der omfatter principperne for databeskyttelse, er klart defineret som et første skridt i den videre udvikling af et sådant instrument.

16. Med hensyn til anvendelsesområdet er de vigtige spørgsmål, der skal besvares:

— hvem er de involverede aktører inden for og uden for retshåndhævelsesområdet?

— hvad er meningen med »med henblik på retshåndhævelse« i forhold til andre formål som f.eks. national sikkerhed og mere specifikt grænsekontrol og folkesundhed?

— hvordan passer instrumentet ind i forbindelse med et globalt transatlantisk sikkerhedsområde?

17. Definitionen af arten skal klarlægge følgende spørgsmål:

— hvis det er relevant, under hvilken søjle instrumentet skal forhandles

— hvorvidt instrumentet skal være bindende for EU og USA

— hvorvidt det skal indebære umiddelbar anvendelighed i den forstand, at det indeholder rettigheder og forpligtelser for de enkelte borgere, der kan håndhæves ved en judiciel myndighed

— hvorvidt instrumentet selv skal give mulighed for udveksling af oplysninger eller fastsætte en minimumsstandard for udveksling af oplysninger, der skal suppleres af særlige aftaler

— hvordan instrumentet skal hænge sammen med eksisterende instrumenter: skal det overholde, erstatte eller supplere dem?

III. 1. **Instrumentets anvendelsesområde**

Involverede aktører

18. Selv om der ikke er nogen klar angivelse i rapporten fra kontaktgruppen på højt plan af det nøjagtige anvendelsesområde for det fremtidige instrument, kan det udledes af de principper, der er nævnt deri, at det påtænkes at dække overførsler både mellem private og offentlige aktører ([7]) og mellem offentlige myndigheder.

— Mellem private og offentlige aktører:

19. Den tilsynsførende ser logikken i at anvende et fremtidigt instrument på overførsler mellem private og offentlige aktører. Udviklingen af et sådant instrument finder sted på baggrund af anmodninger fra USA om oplysninger fra private parter i de senere år. Den tilsynsførende noterer sig således, at private aktører er ved at blive en systematisk kilde til oplysninger i forbindelse med retshåndhævelse, hvad enten det er på EU-plan eller på internationalt plan ([8]). SWIFT-sagen var en afgørende præcedens, hvor en privat virksomhed blev anmodet om systematisk at overføre bulkdata til retshåndhævelsesmyndigheder i en tredjestat ([9]). Indsamling af PNR-data fra luftfartsselskaber følger samme logik. I sin udtalelse om et udkast til rammeafgørelse om et europæisk PNR-system har den tilsynsførende allerede stillet spørgsmålstegn ved lovligheden i denne tendens ([10]).

20. Der er to andre grunde til at være modvillig med hensyn til inddragelsen af overførsler mellem private og offentlige aktører i et fremtidigt instruments anvendelsesområde.

21. For det første kan inddragelsen få en uønsket virkning på EU's eget område. Den tilsynsførende er alvorligt betænkelig for, at hvis data fra private virksomheder (som finansielle institutioner) principielt kan overføres til tredjelande, kan dette fremkalde et stærkt pres for at gøre samme type data tilsvarende tilgængelige inden for EU for retshåndhævelsesmyndigheder. PNR-ordningen er et eksempel på en sådan uheldig udvikling, der startede med USA's bulkindsamling af passageroplysninger, som derefter blev overført til den interne europæiske kontekst ([11]), uden at systemets nødvendighed og proportionalitet er blevet klart påvist.

22. For det andet har den tilsynsførende i sin udtalelse om Kommissionens forslag om EU-PNR også rejst spørgsmålet om databeskyttelsesrammer (første eller tredje søjle), der finder anvendelse på betingelserne for samarbejdet mellem offentlige og private aktører: bør reglerne baseres på kvaliteten i forbindelse med den dataansvarlige (den private sektor) eller på det tilstræbte formål (retshåndhævelse)? Skillelinjen mellem første og tredje søjle er langt fra klar i situationer, hvor der pålægges private aktører forpligtelser til at behandle personoplysninger med henblik på

([7]) Jf. navnlig kapitel 3 i rapporten, Udestående spørgsmål af relevans for transatlantiske forbindelser, punkt 1: Sammenhæng i private enheders forpligtelser under dataoverførsler.

([8]) Jf. i den forbindelse den tilsynsførendes udtalelse af 20. december 2007 om udkastet til forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse, EUT C 110 af 1.5.2008, s. 1. »Der har traditionelt været en klar adskillelse mellem retshåndhævelsesaktiviteter og den private sektors aktiviteter, således at retshåndhævelsesopgaver er blevet udført af særlige myndigheder, især politiet, og den private sektor fra sag til sag er blevet anmodet om at videregive personoplysninger til disse håndhævelsesmyndigheder. Der er nu en tendens til systematisk at pålægge private aktører samarbejde med henblik på retshåndhævelse«.

([9]) Jf. Artikel 29-Gruppens udtalelse 10/2006 af 22. november 2006 om behandling af personoplysninger af Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

([10]) Udtalelse af 20. december 2007, op.cit.

([11]) Jf. forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse nævnt i fodnote 8, som i øjeblikket drøftes i Rådet.

retshåndhævelse. Det er i denne sammenhæng betydningsfuldt, at generaladvokat Bot i sin nylige afgørelse i sagen om lagring af data ([12]) foreslår en afgrænsning for disse situationer, men tilføjer: »Denne afgrænsning kan ganske vist kritiseres og kan i visse henseender synes kunstig.« Den tilsynsførende noterer sig også, at Domstolens PNR-dom ([13]) ikke fuldt ud besvarer spørgsmålet om den gældende retlige ramme. For eksempel betyder det forhold, at visse aktiviteter ikke er dækket af direktiv 95/46/EF, ikke automatisk, at disse aktiviteter kan reguleres under tredje søjle. Som et resultat efterlader det muligvis et smuthul med hensyn til den lov, der skal anvendes, og fører under alle omstændigheder til retsusikkerhed med hensyn til de retlige garantier, der findes for de registrerede.

23. I denne sammenhæng understreger den tilsynsførende, at det må sikres, at et fremtidigt instrument med almindelige databeskyttelsesprincipper ikke som sådan kan legitimere transatlantisk overførsel af personoplysninger mellem private og offentlige parter. Denne overførsel kan kun indgå i et fremtidigt instrument forudsat at:

— det fremtidige instrument præciserer, at overførslen kun er tilladt, hvis det har vist sig, at den er strengt nødvendig for et specifikt formål, hvilket skal afgøres i hvert enkelt tilfælde.

— overførslen selv er omgivet af sikkerhedsgarantier for høj databeskyttelse (som beskrevet i denne udtalelse).

Den tilsynsførende noterer sig desuden usikkerheden med hensyn til de gældende databeskyttelsesrammer og ønsker derfor under alle omstændigheder ikke at inddrage overførsel af personoplysninger mellem private og offentlige parter under den aktuelle EU-lovgivning.

— Mellem offentlige myndigheder:

24. Det nøjagtige sigte med informationsudvekslingen er uklart. Som et første skridt i det videre arbejde hen imod et fælles instrument skal det påtænkte anvendelsesområde for et sådant instrument præciseres. Det er stadig et spørgsmål, hvorvidt

— instrumentet for så vidt angår databaser i EU skal tage sigte på centraliserde databaser, der (delvis) forvaltes af EU, f.eks. Europols og Eurojusts databaser, eller decentraliserede databaser, der forvaltes af medlemsstaterne, eller begge

— instrumentets anvendelsesområde udvides til sammenkoblede net, dvs. hvorvidt de påtænkte garantier vil dække data, der udveksles mellem medlemsstater eller agenturer i EU såvel som i USA

— instrumentet kun vil dække udveksling mellem databaser på retshåndhævelsesområdet (politi, retsvæsen, eventuel told) eller også andre databaser som f.eks. skattedatabaser

— instrumentet også vil berøre nationale sikkerhedsmyndigheders databaser eller vil tillade disse myndigheder adgang til retshåndhævelsesdatabaser på den anden kontraherende parts område (EU til USA og omvendt)

— instrumentet i hvert enkelt tilfælde vil dække overførsel af oplysninger eller permanent adgang til eksisterende databaser. Denne sidste hypotese vil ganske givet rejse proportionalitetsspørgsmål som uddybet i kapitel V under punkt 3.

Retshåndhævelsesformål

25. Definitionen af formålet med en mulig aftale giver også plads til usikkerhed. Retshåndhævelsesformålene er klart angivet i indledningen samt i første princip, der er knyttet til rapporten, og vil blive yderligere analyseret i kapitel IV i denne udtalelse. Den tilsynsførende noterer sig allerede, at det fremgår af disse erklæringer, at udvekslingen af oplysninger vil fokusere på spørgsmål under tredje søjle, men man kan overveje, om dette blot er et første skridt i retning af bredere informationsudveksling. Det forekommer klart, at formål vedrørende offentlig sikkerhed som nævnt i rapporten omfatter bekæmpelse af terrorisme, organiseret kriminalitet og anden kriminalitet. Men skal det også give mulighed for udveksling af oplysninger af anden offentlig interesse såsom eventuelt risici for folkesundheden?

26. Den tilsynsførende anbefaler at begrænse formålet til præcist defineret databehandling og at begrunde de politiske valg, der fører til en sådan definition af formålet.

([12]) Afgørelse fra generaladvokat Bot fremsat den 14. oktober 2008, Irland mod Europa-Parlamentet og Rådet (Sag C-301/06), præmis 108.

([13]) Domstolens dom af 30. maj 2006, Europa-Parlamentet mod Rådet for Den Europæiske Union (C-317/04) og Kommissionen for De Europæiske Fællesskaber (C-318/04), forenede sager C-317/04 og C-318/04, Sml. 2006, s. I-4721.

Et globalt transatlantisk sikkerhedsområde

27. Denne rapports brede sigte skal ses i perspektivet af det globale transatlantiske sikkerhedsområde, der drøftes i den såkaldte »Fremtidsgruppe« ([14]). Denne gruppes rapport, der blev fremlagt i juni 2008, sætter fokus på den eksterne dimension af politikken vedrørende indre anliggender. Den taler for, at EU »*senest i 2014 bør træffe beslutning med hensyn til det politiske mål om at oprette et Euro-atlantisk samarbejdsområde med De Forenede Stater vedrørende frihed, sikkerhed og retfærdighed*«. Et sådant samarbejde vil række ud over sikkerhed i ordets egentlige forstand og vil mindst inddrage de emner, der behandles i det nuværende afsnit IV i EF-traktaten, f.eks. immigration, visum og asyl og samarbejde om civilretlige spørgsmål. Der bør sættes spørgsmålstegn ved, i hvor stort omfang en aftale om grundlæggende databeskyttelsesprincipper som dem, der nævnes i rapporten fra kontaktgruppen på højt plan, kan og skal danne grundlag for udveksling af oplysninger på så bredt et område.

28. Normalt vil søjlestrukturen ikke findes længere i 2014, og der vil være ét retsgrundlag for databeskyttelse inden for EU (under Lissabontraktaten, artikel 16 i traktaten om Den Europæiske Unions funktionsmåde). Det forhold, at der er harmonisering på EU-niveau med hensyn til *regulering* af databeskyttelse, betyder imidlertid ikke, at enhver aftale med et tredjeland giver mulighed for *overførsel* af alle personoplysninger uanset formålet. Afhængigt af sammenhængen og betingelserne for behandling kan der blive behov for tilpassede databeskyttelsesgarantier for visse områder som f.eks. retshåndhævelse. Den tilsynsførende anbefaler at tage konsekvenserne af disse forskellige perspektiver i betragtning i forbindelse med udarbejdelsen af en fremtidig aftale.

III.2. **Aftalens art**

De europæiske institutionelle rammer

29. I hvert fald på kort sigt er det vigtigt at fastslå, under hvilken søjle ordningen skal forhandles. Dette er særlig nødvendigt på grund af de interne rammebestemmelser for databeskyttelse, der vil blive påvirket af en sådan aftale. Vil rammen blive første søjle — især direktiv 95/46/EF med dets specifikke ordning for overførsel af oplysninger til tredjelande — eller vil det blive tredje søjle med en mindre stigende ordning for overførsler til tredjelande? ([15])

30. Selv om retshåndhævelsesformålene er fremherskende, nævner rapporten fra kontaktgruppen på højt plan ikke desto mindre indsamling af oplysninger fra private aktører, og formålene kan også fortolkes bredt, så de rækker ud over ren sikkerhed, herunder f.eks. indvandrings- og grænsekontrolspørgsmål, men eventuelt også folkesundhed. I betragtning af disse usikkerhedsfaktorer vil det absolut være at foretrække at vente på harmoniseringen af søjlerne under EU-lovgivningen som fastsat i Lissabontraktaten for klart at fastlægge retsgrundlaget for forhandlingerne og den præcise rolle, som de europæiske institutioner, navnlig Europa-Parlamentet og Kommissionen, skal spille.

Instrumentets bindende karakter

31. Det bør gøres klart, hvorvidt konklusionerne på drøftelserne skal føre til et memorandum eller et andet ikke-bindende instrument, eller om der skal være tale om en bindende international aftale.

32. Den tilsynsførende foretrækker ligesom rapporten en bindende aftale. En officiel bindende aftale er efter den tilsynsførendes mening en uomgængelig forudsætning for enhver dataoverførsel uden for EU, uanset formålet med at overføre oplysningerne. Der kan ikke finde overførsel af oplysninger til et tredjeland sted uden passende betingelser og sikkerhedsgarantier, der indgår i en specifik (og bindende) retlig ramme. Med andre ord kan et memorandum eller et andet ikke-bindende instrument være nyttigt som vejledning for forhandlinger om yderligere bindende aftaler, men kan aldrig erstatte behovet for en bindende aftale.

Direkte virkning

33. Instrumentets bestemmelser skal være bindende både for USA og for EU og dets medlemsstater.

34. Det bør endvidere sikres, at personer er i stand til at udøve deres rettigheder og navnlig opnå erstatning på grundlag af de vedtagne principper. Efter den tilsynsførendes mening kan dette resultat bedst opnås, hvis instrumentets vigtige bestemmelser formuleres på en sådan måde, at de får direkte virkning for personer, der opholder sig i EU, og kan påberåbes ved en domstol. Den direkte virkning af bestemmelserne i den internationale aftale samt bestemmelserne for dens indarbejdelse i intern europæisk og national lovgivning for at sikre foranstaltningernes effektivitet skal derfor præciseres i instrumentet.

Forholdet til andre instrumenter

35. Det er også et grundlæggende spørgsmål, i hvilken grad aftalen står alene eller skal suppleres i hvert enkelt tilfælde af yderligere aftaler om specifikke udvekslinger af oplysninger. Det er i høj grad diskutabelt, om en enkelt aftale på en relevant måde med et enkelt sæt standarder kan dække de mange specificiteter ved databeskyttelse under tredje søjle. Det er endnu mere tvivlsomt, om den uden yderligere drøftelser og sikkerhedsgarantier kan give

([14]) Rapport fra Den Uformelle Rådgivende Højniveaugruppe om Fremtiden for den Europæiske Politik vedrørende Indre Anliggender, »Frihed, sikkerhed, privatlivets fred — europæiske indre anliggender i en åben verden«, juni 2008, tilgængelig på register.consilium.europa.eu

([15]) Jf. artikel 11 og 13 i rammeafgørelsen om databeskyttelse, der er nævnt i punkt 7 i denne udtalelse.

mulighed for en blankogodkendelse af enhver overførsel af personoplysninger uanset formålet med og arten af de pågældende oplysninger. Aftaler med tredjelande er i øvrigt ikke nødvendigvis permanente, eftersom de kan knyttes til specifikke trusler, underkastes revision og gøres til genstand for »sunset clauses«. På den anden side kan fælles minimumsstandarder, der er anerkendt i et bindende instrument, lette alle yderligere drøftelser om overførsel af personoplysninger i forbindelse med en specifik database eller databehandling.

36. Den tilsynsførende vil derfor gå ind for udviklingen af et sæt minimumskriterier for databeskyttelse, der i hvert enkelt tilfælde suppleres med yderligere specifikke bestemmelser som nævnt i rapporten fra kontaktgruppen på højt plan, snarere end for alternativet med en enkeltstående aftale. Disse supplerende specifikke bestemmelser er en forudsætning for at muliggøre overførsel af oplysninger i et specifikt tilfælde. Dette vil befordre en harmoniseret tilgang for så vidt angår databeskyttelse.

Anvendelse i forhold til eksisterende instrumenter

37. Det bør også undersøges, hvordan en eventuel overordnet aftale kan kombineres med allerede eksisterende aftaler, der er indgået mellem EU og USA. Det bør noteres, at disse eksisterende aftaler ikke har samme bindende karakter: i særlig grad skal nævnes PNR-aftalen (det er den, der indebærer den største retssikkerhed), Europol- og Eurojustaftalerne eller udvekslingen af skrivelser vedrørende SWIFT ([16]). Vil en ny overordnet ramme supplere disse eksisterende instrumenter, eller vil de forblive urørte ved, at den nye ramme kun finder anvendelse på andre fremtidige udvekslinger af personoplysninger? Efter den tilsynsførendes mening kræver juridisk kohærens et harmoniseret sæt regler, der gælder for og supplerer både eksisterende og fremtidige bindende aftaler om overførsler af oplysninger.

38. Anvendelsen af den overordnede aftale på eksisterende instrumenter vil have den fordel, at deres bindende karakter bliver styrket. Dette vil især være særlig velkomment med hensyn til instrumenter, der ikke er retligt bindende, f.eks. udvekslingen af skrivelser vedrørende SWIFT, eftersom det i det mindste vil pålægge overholdelse af en række generelle principper til beskyttelse af privatlivets fred.

IV. **GENEREL JURIDISK EVALUERING**

39. I dette kapitel ses der på, hvordan en specifik rammes eller et specifikt instruments beskyttelsesniveau skal vurderes, herunder spørgsmålet om de benchmarks, der skal anvendes, og de nødvendige grundlæggende krav.

([16]) Jf. fodnote 2.

Passende beskyttelsesniveau

40. Efter den tilsynsførendes opfattelse skal det stå klart, at et af de vigtigste resultater af et fremtidigt instrument vil være, at overførsel af personoplysninger til USA kun kan finde sted i det omfang, de amerikanske myndigheder garanterer et passende beskyttelsesniveau (og omvendt).

41. Den tilsynsførende mener, at kun en virkelig test af et tilstrækkeligt beskyttelsesniveau kan give tilstrækkelige garantier med hensyn til niveauet for beskyttelse af personoplysninger. Han mener, at en overordnet rammeaftale med et anvendelsesområde så bredt som det, kontaktgruppen på højt plan opererer med i sin rapport, vil få vanskeligheder med som sådan at bestå en virkelig tilstrækkelighedstest. Den overordnede aftales tilstrækkelige beskyttelsesniveau kan kun anerkendes, hvis det kombineres med tilstrækkelige beskyttelsesniveauer i specifikke aftaler, der er indgås i hvert enkelt tilfælde.

42. Vurderingen af beskyttelsesniveauet i tredjelande er ikke en usædvanlig øvelse, navnlig ikke for Europa-Kommissionen: et tilstrækkeligt beskyttelsesniveau er under første søjle et krav for overførsel. Det er blevet målt ved flere lejligheder i henhold til artikel 25 i direktiv 95/46 på grundlag af specifikke kriterier og bekræftet ved afgørelser truffet af Europa-Kommissionen ([17]). Under tredje søjle er der ikke udtrykkeligt forudset et sådant system: målingen af et tilstrækkelig beskyttelsesniveau foreskrives kun i den specifikke situation, der er omhandlet i artikel 11 og 13 i den — endnu ikke vedtagne — rammeafgørelse om databeskyttelse ([18]), og overlades til medlemsstaterne.

43. I dette tilfælde berører øvelsen retshåndhævelsesformål, og drøftelserne føres af Kommissionen under Rådets tilsyn. Konteksten er forskellig fra evalueringen af safe harbor-principperne eller den canadiske lovgivnings tilstrækkelige beskyttelseniveau og har flere forbindelser med de seneste PNR-forhandlinger med USA og Australien, som fandt sted i en retlig ramme under tredje søjle. Kontaktgruppen på højt plans principper er imidlertid også blevet nævnt i forbindelse med visumfritagelsesprogrammet, der vedrører grænse og indvandring og dermed spørgsmål under første søjle.

44. Den tilsynsførende anbefaler, at enhver konstatering vedrørende et tilstrækkeligt beskyttelsesniveau under et fremtidigt instrument bør bygge på erfaringer på disse forskellige

([17]) Kommissionens afgørelser om tilstrækkeligheden af beskyttelsen af personoplysninger i tredjelande, herunder Argentina, Canada, Schweiz, De Forenede Stater, Guernsey, Isle of Man og Jersey, er tilgængelige på http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Begrænset til en medlemsstats overførsel til et tredjeland eller en international instans af oplysninger modtaget fra en kompetent myndighed i en anden medlemsstat.

områder. Han anbefaler videreudvikling af begrebet »tilstrækkeligt beskyttelsesniveau« i forbindelse med et fremtidigt instrument på grundlag af lignende kriterier som anvendt i tidligere konstateringer af et tilstrækkeligt beskyttelsesniveau.

Gensidig anerkendelse — gensidighed

45. Et andet element i forbindelse med beskyttelsesniveauet vedrører gensidig anerkendelse af EU's og USA's systemer. Rapporten fra kontaktgruppen på højt plan nævner i den forbindelse, at målet vil være at opnå anerkendelse af effektiviteten i hinandens systemer om beskyttelse af privatlivets fred og databeskyttelse på de områder, der er dækket af disse principper ([19]), og at nå tilsvarende og gensidig anvendelse af lovgivning om beskyttelse af privatlivets fred og personoplysninger.

46. Den tilsynsførende finder det indlysende, at gensidig anerkendelse (eller gensidighed) kun er mulig, hvis der sikres et passende beskyttelsesniveau. Med andre ord bør det fremtidige instrument harmonisere et minimumsbeskyttelsesniveau (ved en konstatering af et tilstrækkeligt beskyttelsesniveau under hensyntagen til behovet for specifikke aftaler i hvert enkelt tilfælde). Kun hvis denne forhåndsbetingelse er opfyldt, kan gensidigheden blive anerkendt.

47. Det første element, der skal tages i betragtning, er gensidigheden i materielle bestemmelser om databeskyttelse. Efter den tilsynsførendes mening bør en aftale omhandle begrebet gensidighed for så vidt angår materielle bestemmelser om databeskyttelse på en måde, der på den ene side sikrer, at databehandling på EU's område (og USA) fuldt ud overholder national lovgivning om databeskyttelse, og på den anden side, at behandling uden for oplysningernes oprindelsesland og inden for aftalens anvendelsesområde overholder principperne om databeskyttelse som fastlagt i aftalen.

48. Det andet element er gensidighed i klageprocedurerne. Det bør sikres, at europæiske borgere har passende klagemuligheder, når oplysninger om dem bliver behandlet i USA (uanset den lovgivning, der gælder for denne behandling), men også at Den Europæiske Union og dets medlemsstater giver tilsvarende rettigheder til amerikanske borgere.

49. Det tredje element er gensidighed i forbindelse med retshåndhævelsesmyndigheders adgang til personoplysninger. Hvis et instrument giver de amerikanske myndigheder adgang til oplysninger med oprindelse i Den Europæiske Union, vil gensidigheden medføre, at samme adgang skal gives til EU's myndigheder i forbindelse med oplysninger med oprindelse i USA. Gensidigheden må ikke skade effektiviteten af beskyttelsen af den registrerede. Dette er en forudsætning for at tillade »transatlantisk« adgang for retshåndhævelsesmyndighederne. Dette betyder helt konkret følgende:

— Amerikanske myndigheders direkte adgang til oplysninger på EU's område (og omvendt) skal ikke være tilladt. Adgang gives kun på et indirekte grundlag under et push-system.

— Denne adgang skal finde sted under kontrol fra databeskyttelsesmyndigheder og retslige myndigheder i det land, hvor databehandlingen finder sted.

— Amerikanske myndigheders adgang til databaser i EU skal overholde de materielle bestemmelser om databeskyttelse (se ovenfor) og sikre fuld klagemulighed for den registrerede.

Instrumentets præcision

50. Specifikationen af betingelserne for vurderingen (konstatering vedrørende tilstrækkeligt beskyttelsesniveau, ækvivalens, gensidig anerkendelse) er meget vigtig, eftersom den fastlægger indholdet for så vidt angår præcision, retssikkerhed og beskyttelsens effektivitet. Indholdet af et fremtidigt instrument skal være præcist og nøjagtigt.

51. Det bør desuden være klart, at enhver specifik aftale, der indgås på et senere trin, stadig skal indeholde detaljerede og fuldstændige databeskyttelsesgarantier i forhold til genstanden for den påtænkte udveksling af oplysninger. Kun et sådant dobbelt niveau af konkrete databeskyttelsesprincipper kan sikre den nødvendige »tætte forbindelse« mellem den overordnede aftale og specifikke aftaler, som det allerede er anført i punkt 35 og 36 i denne udtalelse.

Udvikle en model for andre tredjelande

52. Det omfang, i hvilket en aftale med USA kan blive en model for andre tredjelande, fortjener særlig opmærksomhed. Den tilsynsførende noterer sig, at ovennævnte rapport fra Fremtidsgruppen foruden USA også nævner Rusland som en strategisk partner for EU. For så vidt principperne er neutrale og i overensstemmelse med grundlæggende EU-sikkerhedsgarantier, kan de udgøre en nyttig præcedens. Specificiteter i forbindelse med f.eks. modtagerlandets retlige ramme eller formålet med overførslen vil forhindre ren overtagelse af aftalen. Tilsvarende afgørende vil tredjelandes demokratiske situation være: det bør sikres, at de principper, der er opnået enighed om, vil blive effektivt garanteret og gennemført i modtagerlandet.

Hvilke benchmarks bruges til at vurdere beskyttelsesniveauet?

53. En implicit eller eksplicit konstatering vedrørende et tilstrækkeligt beskyttelsesniveau skal under alle omstændigheder overholde internationale og europæiske retlige

([19]) Kapitel A. Bindende international aftale, s. 8.

rammer og navnlig de i fællesskab vedtagne databeskyttelsessikkerhedsgarantier. Disse er sikret i FN's retningslinjer, i Europarådets konvention 108 og dens tillægsprotokol, i OECD's retningslinjer og i udkastet til rammeafgørelse om databeskyttelse samt for aspekter vedrørende første søjle i direktiv 95/46/EF ([20]). Alle disse instrumenter indeholder lignende principper, der er mere bredt anerkendt som kernen i beskyttelsen af personoplysninger.

54. Det er således meget vigtigt, at der bliver taget behørigt hensyn til ovennævnte principper i betragtning af virkningerne af en potentiel aftale som den, der er omtalt i rapporten fra kontaktgruppen på højt plan. Med et instrument, der vedrører hele *håndhævelsesområdet* i et tredjeland, vil der virkelig foreligge en situation uden fortilfælde. Eksisterende afgørelser om konstatering vedrørende et tilstrækkeligt beskyttelsesniveau i første søjle og aftaler indgået med tredjelande under EU's tredje søjle (Europol, Eurojust) har altid været knyttet til en specifik overførsel af oplysninger, mens overførsler med et meget bredere omfang her vil kunne blive mulige i betragtning af det brede formål, der tilstræbes (bekæmpelse af lovovertrædelser, national og offentlig sikkerhed, grænsehåndhævelse) og det ukendte antal berørte databaser.

Grundlæggende krav

55. De betingelser, der skal opfyldes i forbindelse med overførsel af personoplysninger til tredjelande, er blevet fastlagt i et arbejdsdokument fra Artikel 29-Gruppen ([21]). Enhver aftale om minimumsprincipper for privatlivets fred skal gennem en test, der skal vise, at den opfylder kravene og sikrer effektiviteten af databeskyttelsessikkerhedsgarantierne.

— Om substansen: databeskyttelsesprincipperne bør sikre et højt beskyttelsesniveau og opfylde standarderne i overensstemmelse med EU-principperne. De 12 principper, der indgår i rapporten for kontaktgruppen på højt plan, vil i den forbindelse blive yderligere analyseret i kapitel V i denne udtalelse.

— Om specificitet: afhængigt af aftalens art, og navnlig hvis den udgør en officiel international aftale, skal reglerne og procedurerne være tilstrækkeligt detaljerede til at muliggøre en effektiv gennemførelse

— Om tilsyn: for at sikre overholdelse af de vedtagne regler skal der indføres kontrolmekanismer, både internt (audit) og eksternt (revision). Disse mekanismer skal være tilgængelige for begge parter i aftalen. Tilsyn omfatter mekanismer til at sikre overholdelse på makroniveau, f.eks. fælles revisionsmekanismer, samt overholdelse på mikroniveau, f.eks. individuelle klagemuligheder.

56. Ud over disse tre grundlæggende krav skal der lægges særlig vægt på de specifikke forhold i forbindelse med behandling af personoplysninger i en retshåndhævelseskontekst. Dette er nemlig et område, hvor grundlæggende rettigheder kan udsættes for begrænsninger. Der skal derfor vedtages sikkerhedsgarantier for at kompensere for personers rettigheder, navnlig med hensyn til følgende aspekter i betragtning af virkningerne for personen:

— Gennemsigtighed: information og adgang til personoplysninger kan begrænses i en retshåndhævelseskontekst, f.eks. af hensyn til diskrete undersøgelser. Mens der inden for EU traditionelt anvendes supplerende mekanismer for at kompensere for denne begrænsning af grundlæggende rettigheder (der ofte involverer uafhængige databeskyttelsesmyndigheder), må det sikres, at lignende kompensationsmekanismer er til rådighed, når oplysningerne overføres til et tredjeland.

— Klageadgang: af ovennævnte årsager skal enkeltpersoner nyde godt af alternative muligheder til at få forsvaret deres rettigheder, navnlig gennem en uafhængig tilsynsmyndighed og for en domstol.

— Opbevaring af data: begrundelsen for perioden for opbevaring af data er muligvis ikke gennemsigtig. Der må træffes foranstaltninger, således at dette ikke forhindrer de registreredes eller tilsynsmyndighedernes effektive udøvelse af rettigheder.

([20]) — De Forenede Nationers retningslinjer vedrørende edb-databaser med personoplysninger, vedtaget af Generalforsamlingen den 14. december 1990, tilgængelige på www.unhchr.ch/html/menu3/b/71.htm
— Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger af 28. januar 1981, tilgængelig på http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm
— OECD: Retningslinjer for beskyttelse af privatlivets fred og overførsel af personoplysninger mellem landene vedtaget den 23. september 1980, tilgængelige på www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Udkast til Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, tilgængeligt på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— Europa-Parlamentets og Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EFT L 281 af 23.11.1995, s. 31.

([21]) Arbejdsdokument af 24. juli 1998 om overførsel af personoplysninger til tredjelande: Anvendelse af artikel 25 og 26 i EU's databeskyttelsesdirektiv; WP12.

— Retshåndhævelsesmyndigheders klare ansvarsforhold: hvis der ikke er effektiv gennemsigtighed, kan enkeltpersoners eller institutionelle interessenters kontrolmekanismer på ingen måde blive omfattende. Det vil stadig være yderst vigtigt, at der etableres en sådan kontrol i betragtning af oplysningernes følsomhed og de tvangsforanstaltninger, der kan træffes over for enkeltpersoner på grundlag af databehandlingen. Klare ansvarsforhold er et afgørende spørgsmål for så vidt angår nationale kontrolmekanismer i modtagerlandet, men også for så vidt angår revisionsmuligheder for oplysningernes oprindelsesland eller -region. Sådanne revisionsmekanismer er fastsat i specifikke aftaler som f.eks. PNR-aftalen, og den tilsynsførende anbefaler kraftigt, at de ligeledes medtages i det overordnede instrument.

V. **ANALYSE AF PRINCIPPERNE**

Indledning

57. I dette kapitel analyseres de 12 principper, der er omhandlet i dokumentet fra kontaktgruppen på højt plan ud fra følgende synsvinkel:

— Disse principper viser, at USA og EU har nogle fælles synspunkter for så vidt angår principperne, ligesom der kan noteres ligheder med principperne i konvention 108.

— Enighed om principperne er dog ikke nok. Et retligt instrument skal være stærkt nok til at sikre overensstemmelse.

— Den tilsynsførende beklager, at principperne ikke ledsages af en begrundelse.

— Det bør stå klart, inden principperne beskrives, at begge parter har samme forståelse af det ordvalg, der anvendes f.eks. med hensyn til personoplysninger eller beskyttede personer. Definitioner heraf vil være velkomne.

1. Specifikation af formål

58. Det første princip, der er anført i bilaget til rapporten fra kontaktgruppen på højt plan, går ud på, at personoplysninger skal behandles som led i retshåndhævelse. Som nævnt ovenfor refererer dette for Den Europæiske Union til forebyggelse, afsløring, efterforskning og retsforfølgning af strafbare handlinger. For USA går fortolkningen af retshåndhævelse dog ud over strafbare handlinger og omfatter »grænseoverskridende retshåndhævelse, offentlig sikkerhed og nationale sikkerhedsbehov«. Følgerne af sådanne uoverensstemmelser mellem EU's og USA's erklærede formål er ikke klare. Mens rapporten nævner, at formålene i praksis i vidt omfang kan være sammenfaldende, er det dog stadig afgørende at vide, præcist i hvilket omfang de *ikke* er sammenfaldende. På retshåndhævelsesområdet skal princippet om begrænsning af formålet overholdes strengt i betragtning af de følger, de trufne foranstaltninger har for enkeltpersoner, og de erklærede formål skal være klare og afgrænsede. Under hensyn til den i rapporten nævnte gensidighed forekommer tilnærmelsen af disse formål også meget vigtig. Kort sagt er der behov for en præcisering af opfattelsen af dette princip.

2. Oplysningernes integritet/pålidelighed

59. Den tilsynsførende ser med tilfredshed på bestemmelsen, ifølge hvilken nøjagtige, relevante, rettidige og fuldstændige personoplysninger som nødvendige for lovlig behandling. Et sådant princip er en grundlæggende betingelse for al effektiv databehandling.

3. Nødvendighed/proportionalitet

60. Princippet etablerer en klar forbindelse mellem indsamlede oplysninger og nødvendigheden af disse oplysninger for at gennemføre et retshåndhævelsesformål, der er fastlagt i loven. Dette krav om et retligt grundlag er et positivt element med henblik på at fastslå behandlingens lovlighed. Den tilsynsførende noterer sig imidlertid, at selv om dette styrker retssikkerheden i behandlingen, udgøres retsgrundlaget for en sådan behandling af en lov i et tredjeland. En lov i et tredjeland kan ikke i sig selv udgøre et legitimt grundlag for en overførsel af personoplysninger ([22]). I forbindelse med rapporten fra kontaktgruppen på højt plan antages det, at lovligheden af loven i et tredjeland, dvs. USA, principielt anerkendes. Der erindres om, at hvis dette ræsonnement kan være berettiget her ud fra den betragtning, at USA er en demokratisk stat, vil samme ordning ikke kunne gælde for eller overføres på forbindelserne med andre tredjelande.

61. Enhver overførsel af personoplysninger skal være relevant, nødvendig og hensigtsmæssig ifølge bilaget til rapporten fra kontaktgruppen på højt plan. Den tilsynsførende understreger, at behandlingen for at stå i rimeligt forhold til formålet ikke må være uberettiget forstyrrende, og de nærmere bestemmelser for behandlingen skal være afbalancerede og tage hensyn til de registrerede personers rettigheder og interesser.

62. Derfor skal der gives adgang til oplysninger fra sag til sag afhængig af praktiske behov i forbindelse med en specifik undersøgelse. Permanent adgang for tredjelandes retshåndhævelsesmyndigheder til databaser i EU vil anses for ude af proportion og utilstrækkeligt begrundet. Den tilsynsførende minder om, at selv i forbindelse med eksisterende aftaler om udveksling af oplysninger, f.eks. PNR-aftalen,

([22]) Jf. direktiv 95/46/EF, særlig artikel 7, litra c) og e). I sin udtalelse nr. 6/2002 af 24. oktober 2002 om videregivelse af passagerlisteoplysninger og andre oplysninger fra luftfartsselskaber til USA anførte Artikel 29-Gruppen, at det ikke forekommer acceptabelt, at en ensidig afgørelse truffet af et tredjeland af hensyn til dets egne offentlige interesser skal føre til rutinemæssig overførsel i stor målestok af oplysninger, der er beskyttet i henhold til direktivet.

er udvekslingen af oplysninger baseret på specifikke omstændigheder og afsluttes efter en begrænset periode ([23]).

63. Ud fra samme tankegang bør perioden for opbevaring af data reguleres: data skal kun opbevares, så længe de er nødvendige i betragtning af det specifikke formål, der følges. Hvis de ikke længere er relevante i forhold til det fastlagte formål, skal de slettes. Den tilsynsførende er stærkt imod oprettelsen af datavarehuse, hvor oplysninger om ikke-mistænkte personer lagres med henblik på et eventuelt senere behov.

4. Informationssikkerhed

64. Foranstaltninger og procedurer for at sikre oplysninger mod misbrug, ændringer og andre risici er angivet i principperne såvel som en bestemmelse om begrænsning af adgangen til autoriserede personer. Den tilsynsførende finder dette tilfredsstillende.

65. Princippet kan desuden suppleres med en bestemmelse om, at der bør føres log over dem, der får adgang til oplysningerne. Det vil styrke sikkerhedsgarantiernes effektivitet at begrænse adgang og forhindre misbrug af oplysningerne.

66. Gensidig underretning bør desuden forudses i tilfælde af sikkerhedsbrud: modtagere i USA såvel som i EU vil være ansvarlige for at underrette deres modparter, hvis oplysninger, de modtager, har været genstand for uretmæssig videregivelse. Dette vil bidrage til at øge ansvaret for en sikker databehandling.

5. Særlige kategorier af personoplysninger

67. Princippet om forbud mod behandling af følsomme oplysninger er efter den tilsynsførendes mening kraftigt svækket af den undtagelse, der tillader behandling af følsomme oplysninger, for hvilke national lov giver »passende sikkerhed«. Netop på grund af oplysningernes følsomme karakter skal enhver fravigelse af forbudsprincippet begrundes passende og præcist med en liste over formål og omstændigheder, under hvilke en udpeget type følsomme oplysninger kan behandles, samt med en angivelse af, hvilke registeransvarlige der kan behandle denne type oplysninger. Blandt de beskyttelsesgarantier, der skal vedtages, finder den tilsynsførende, at følsomme oplysninger ikke skal udgøre et sådant element, der kan udløse en undersøgelse. De kan være til rådighed under specifikke omstændigheder, men kun som supplerende information vedrørende en registreret, der allerede er genstand for undersøgelse. Disse beskyttelsesgarantier og betingelser skal specificeres på en begrænsende måde i affattelsen af princippet.

6. Klare ansvarsforhold

68. Som omhandlet i punkt 55-56 i denne udtalelse skal klare ansvarsforhold effektivt sikres for offentlige enheder, der behandler personoplysninger, og der skal i aftalen gives garanti for den måde, hvorpå disse ansvarsforhold sikres. Dette er særligt vigtigt i betragtning af den mangel på gennemsigtighed, der traditionelt forbindes med behandlingen af personoplysninger i en retshåndhævelseskontekst. På denne baggrund er det ikke en tilfredsstillende garanti at nævne — som det er tilfældet nu i bilaget — at offentlige enheder skal være ansvarlige uden at give yderligere forklaring på de nærmere retningslinjer for og følgerne af et sådant ansvarsforhold. Den tilsynsførende anbefaler, at der gives en sådan forklaring i teksten til instrumentet.

7. Uafhængigt og effektivt tilsyn

69. Den tilsynsførende støtter fuldt ud medtagelsen af en bestemmelse om uafhængigt og effektivt tilsyn fra en eller flere offentlige tilsynsmyndigheder. Han mener, at det bør gøres klart, hvordan uafhængighed fortolkes, navnlig hvem disse myndigheder er uafhængige af, og hvem de refererer til. Der er behov for kriterier herfor, der skal tage hensyn til institutionel og funktionel uafhængighed i forhold til de udøvende og lovgivende instanser. Den tilsynsførende minder om, at dette er et vigtigt element for at sikre effektiv overholdelse af de vedtagne principper. Disse myndigheders interventions- og håndhævelsesbeføjelser er også yderst vigtige i forbindelse med spørgsmålet om klare ansvarsforhold for de offentlige enheder, der behandler personoplysninger som nævnt ovenfor. Deres eksistens og beføjelser bør gøres klart synlige for de registrerede, så disse får mulighed for at udøve deres rettigheder, navnlig hvis flere myndigheder er kompetente afhængig af behandlingens kontekst.

70. Den tilsynsførende anbefaler desuden, at en fremtidig aftale også skal omfatte mekanismer for samarbejde mellem tilsynsmyndighederne.

8. Individuel adgang og berigtigelse

71. Der er behov for specifikke garantier, når det drejer sig om adgang og berigtigelse i en retshåndhævelsessammenhæng. I den forbindelse ser den tilsynsførende med tilfredshed på princippet om, at personer skal/bør have adgang og midler til at søge »berigtigelse og/eller sletning af deres personoplysninger«. Der er dog stadig en vis usikkerhed med hensyn til definitionen af personer (alle registrerede bør være beskyttede og ikke kun borgere i det pågældende land) og betingelserne for, at personer kan gøre indsigelse mod behandlingen af deres oplysninger. Det skal præciseres, i hvilke »relevante tilfælde« der kan gøres indsigelse eller ikke. Det bør være klart for de registrerede, under hvilke omstændigheder — afhængig f.eks. af typen af

([23]) Denne aftale udløber og ophører med at gælde syv år fra datoen for undertegnelsen, medmindre begge parter er enige om at erstatte den med en anden.

myndighed, typen af undersøgelse eller andre kriterier — de vil være i stand til at udøve deres rettigheder.

72. Hvis der ikke er nogen direkte mulighed for at gøre indsigelse mod en behandling af berettigede grunde, bør der i øvrigt være mulighed for en indirekte efterprøvning gennem den uafhængige myndighed, der er ansvarlig for tilsynet med behandlingen.

9. Gennemsigtighed og meddelelse

73. Den tilsynsførende understreger endnu en gang betydningen af effektiv gennemsigtighed for at give personer mulighed for at udøve deres rettigheder og bidrage til overordnede klare ansvarsforhold for offentlige myndigheder, der behandler personoplysninger. Han støtter principperne i rapporten og insisterer navnlig på behovet for en generel *og* en individuel meddelelse til den pågældende person. Dette afspejles i princippet i punkt 9 i bilaget til rapporten.

74. Rapporten nævner imidlertid i kapitel 2, del A B (Godkendte principper), at gennemsigtighed i USA kan omfatte individuel eller kombineret offentliggørelse i Federal Register, individuel meddelelse og offentliggørelse i retten. Det skal være klart, at offentliggørelse i en lovtidende ikke er tilstrækkeligt i sig selv til at sikre passende orientering af den registrerede. Ud over behovet for individuel meddelelse minder den tilsynsførende om, at oplysninger skal gives i en form og på et sprog, der let kan forstås af den registrerede.

10. Klageadgang

75. For at sikre effektiv udøvelse af enkeltpersoners rettigheder skal de kunne indgive klage for en uafhængig databeskyttelsesmyndighed samt have et retsmiddel ved en uafhængig og upartisk domstol. Begge klagemuligheder bør være lige tilgængelige.

76. Adgang til en uafhængig databeskyttelsesmyndighed er nødvendig, eftersom det giver en fleksibel og mindre kostbar bistand i en sammenhæng — retshåndhævelse — der kan være temmelig uigennemsigtig for personerne. Databeskyttelsesmyndighederne kan også yde bistand ved at udøve adgangsrettigheder på vegne af registrerede, hvor undtagelser forhindrer sidstnævnte i at få direkte adgang til deres personoplysninger.

77. Adgang til retsvæsenet er en yderligere og central garanti for, at registrerede kan søge klageadgang til en myndighed, der tilhører en gren af det demokratiske system, der er adskilt fra de offentlige institutioner, der faktisk behandler deres oplysninger. De Europæiske Fællesskabers Domstol ([24]) har anset et sådant effektivt retsmiddel ved en domstol for at være af afgørende betydning for at sikre den enkelte en effektiv retsbeskyttelse. Det er udtryk for et almindeligt fællesskabsretligt princip, der ligger til grund for medlemsstaternes fælles forfatningstraditioner, og som har fundet udtryk i artiklerne 6 og 13 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder. Eksistensen af et retsmiddel er også eksplicit fastsat i artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder og i artikel 22 i direktiv (EF) 95/46 uden at foregribe nogen administrativ klageadgang.

11. Edb-baserede individuelle afgørelser

78. Den tilsynsførende ser med tilfredshed på bestemmelsen om passende beskyttelse i tilfælde af edb-baseret behandling af personoplysninger. Han noterer sig, at en fælles forståelse af, hvad der betragtes som en betydelig negativ handling vedrørende enkeltpersonens relevante interesser, vil præcisere betingelserne for anvendelse af dette princip.

12. Videreformidling

79. Betingelserne for videreformidling er uklare for nogles vedkommende. Navnlig når videreformidlingen skal overholde internationale ordninger og aftaler mellem afsenderland og modtagerland, bør det præciseres, om dette henviser til aftaler mellem de to lande, der har indledt den første overførsel, eller de to lande, der er involveret i videreformidlingen. Ifølge den tilsynsførende er der i hvert tilfælde behov for aftaler mellem de to lande, der har indledt den første overførsel.

80. Den tilsynsførende noterer sig en meget bred definition af »legitime offentlige interesser«, der giver mulighed for videreformidling. Omfanget af den offentlige sikkerhed er fortsat uklart, og udvidelsen af overførsler i tilfælde af et etisk brud eller lovregulerede erhverv synes uberettiget og overdreven i forbindelse med retshåndhævelse.

VI. **KONKLUSION**

81. Den tilsynsførende hilser det fælles arbejde velkommen, som EU's og USA's myndigheder har udført på retshåndhævelsesområdet, hvor databeskyttelse er afgørende. Han ønsker dog at insistere på det forhold, at spørgsmålet er komplekst, navnlig med hensyn til det præcise anvendelsesområde og arten, og at det derfor fortjener en omhyggelig og tilbundsgående analyse. Virkningen af et transatlantisk databeskyttelsesinstrument bør nøje overvejes i

([24]) Sag 222/84, *Johnston* [1986] Sml. 1651; Sag 222/86, *Heylens* [1987] Sml. 4097; Sag C-97/91, *Borelli* [1992] Sml. I-6313.

forhold til den eksisterende retlige ramme og følgerne for borgerne.

82. Den tilsynsførende ønsker mere klarhed og konkrete bestemmelser, navnlig om følgende aspekter:

— præcisering af arten af instrumentet, der bør være retligt bindende for at give tilstrækkelig retssikkerhed

— en grundig konstatering af et tilstrækkeligt beskyttelsesniveau baseret på vigtige krav vedrørende substansen, specificiteten og tilsynsaspekterne i ordningen Den tilsynsførende mener, at den generelle aftales tilstrækkelige beskyttelsesniveau kun kan anerkendes, hvis den kombineres med et tilstrækkeligt beskyttelsesniveau ved specifikke aftaler, der indgås i hvert enkelt tilfælde

— et begrænset anvendelsesområde med en klar fælles definition af de retshåndhævelsesformål, der er på spil

— præcisering af de nærmere bestemmelser, ifølge hvilke private enheder kan deltage i dataoverførselsordninger

— overholdelse af proportionalitetsprincippet, der indebærer udveksling af oplysninger fra sag til sag, når der er et konkret behov for det

— stærke tilsynsmekanismer og mekanismer for klageadgang for registrerede, herunder administrativ klageadgang og retsmidler

— effektive foranstaltninger, der garanterer alle registrerede uanset nationalitet udøvelse af deres rettigheder

— inddragelse af uafhængige databeskyttelsesmyndigheder, navnlig i forbindelse med tilsyn og bistand til registrerede.

83. Den tilsynsførende insisterer på det forhold, at hastværk i forbindelse med udarbejdelsen af principperne bør undgås, da det bare vil føre til utilfredsstillende løsninger med de modsatte virkninger af de tilsigtede med hensyn til databeskyttelse. Den bedste vej frem vil derfor på dette stadium være udarbejdelsen af en køreplan med henblik på en mulig aftale på et senere tidspunkt.

84. Den tilsynsførende udbeder sig også mere gennemsigtighed i processen med udarbejdelse af principperne for databeskyttelse. Kun hvis alle interessenter, herunder Europa-Parlamentet, bliver inddraget, kan instrumentet drage fordel af en demokratisk debat og få den nødvendige støtte og anerkendelse.

Udfærdiget i Bruxelles, den 11. november 2008.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Rådet, Europa-Parlamentet og Det Europæiske Økonomiske og Sociale Udvalg — På vej mod en EU-strategi for e-justice

(2009/C 128/02)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser 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]),

som henviser 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 ([2]), særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. Den 30. maj 2008 blev meddelelsen fra Kommissionen til Rådet, Europa-Parlamentet og Det Europæiske Økonomiske og Sociale Udvalg »På vej mod en EU-strategi for e-justice« (i det følgende benævnt »meddelelsen«) vedtaget. I overensstemmelse med artikel 41 i forordning (EF) nr. 45/2001 forelægger den tilsynsførende hermed sin udtalelse.

2. Meddelelsen har til formål at foreslå en strategi for e-justice, der sigter mod at øge borgernes tillid til det europæiske område med retfærdighed. Det væsentligste mål med e-justice bør være at øge retsvæsenets effektivitet overalt i EU til fordel for borgerne. EU's indsats bør på trods af de sproglige, kulturelle og retlige barrierer, som retssystemernes mangfoldighed indebærer, give borgerne mulighed for at få adgang til oplysninger. Et udkast til handlingsplan og en tidsplan for de forskellige projekter er vedlagt meddelelsen.

3. Denne udtalelse fra den tilsynsførende kommenterer meddelelsen, i det omfang den vedrører behandling af personoplysninger, beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og fri udveksling af oplysninger.

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

II. BAGGRUND OG KONTEKST

4. I juni 2007 fastlagde Rådet (retlige og indre anliggender) ([3]) en række prioriteter for udviklingen af e-justice.

— oprettelse af en europæisk grænseflade, e-justice-portalen

— skabelse af forudsætningerne for netværk mellem registre på forskellige områder såsom strafferegistre, insolvensregistre, handels- og virksomhedsregistre og matrikelregistre

— indledning af forberedelserne til brug af ikt i forbindelse med den europæiske betalingspåkravsprocedure

— øget anvendelse af videokonferencer i forbindelse med grænseoverskridende retssager, navnlig i forbindelse med bevisoptagelse

— udvikling af hjælperedskaber til tolkning og oversættelse.

5. Der er siden da gjort stadige fremskridt i arbejdet med e-justice. Efter Kommissionens opfattelse skal det arbejde, der udføres på dette område, sikre, at operationelle projekter og decentrale strukturer prioriteres, samtidig med at der sikres en koordinering på EU-plan, idet der arbejdes på grundlag af de bestående retsakter og anvendes it-redskaber til at forbedre deres effektivitet. Europa-Parlamentet har også givet udtryk for støtte til e-justice-projektet ([4]).

6. Kommissionen har til stadighed tilskyndet til brug af moderne informationsteknologi, både på det civilretlige og på det strafferetlige område. Dette har ført til instrumenter som f.eks. det europæiske betalingspåkrav. Kommissionen har siden 2003 administreret portalen for Det Europæiske Retlige Netværk for Civil- og Handelssager, som er tilgængelig for borgerne på 22 sprog. Kommissionen har også udarbejdet og indført Det Europæiske Retlige Atlas. Disse redskaber er forberedende elementer til en fremtidig EU-ramme for e-justice. På det strafferetlige område har Kommissionen arbejdet på at udvikle et redskab, der kan muliggøre udveksling af oplysninger fra medlemsstaternes strafferegistre ([5]). Ikke kun Kommissionen men også Eurojust har udviklet en række sikre kommunikationssystemer med nationale myndigheder.

([3]) Dok. 10393/07 JURINFO 21.
([4]) Jf. udkastet til Europa-Parlamentets betænkning, Retsudvalget.
([5]) Jf. navnlig det nedenfor omhandlede ECRIS-system.

7. E-justice sigter mod at byde på mange muligheder, som kan give borgerne en mere konkret opfattelse af det europæiske retlige område i de kommende år. Med henblik på at opstille en overordnet strategi for dette vigtige område, vedtog Kommissionen denne meddelelse om e-justice. I meddelelsen fastlægges der objektive prioriteringskriterier, navnlig for fremtidige projekter på EU-plan, så der inden for en rimelig tid kan opnås konkrete resultater.

8. Arbejdsdokument fra Kommissionens tjenestegrene, et ledsagedokument til meddelelsen med et resumé af konsekvensanalysen, giver også en del baggrundsinformation ([6]). Konsekvensanalyserapporten er blevet udarbejdet under hensyntagen til medlemsstaternes, retsmyndighedernes, retsvæsenets aktørers, borgernes og erhvervslivets reaktioner. Den tilsynsførende er ikke blevet hørt. Konsekvensanalyserapporten henviste til en politisk option med henblik på at afhjælpe de problemer, der kombinerer EU-dimensionen med den nationale kompetence. Meddelelsen går ind for denne option. Strategien vil fokusere på anvendelse af videokonferencer, oprettelse af en e-justice-portal, forbedring af oversættelsesmulighederne gennem udvikling af online-oversættelsesredskaber, forbedring af kommunikationen mellem retsmyndighederne, øget sammenkobling af nationale registre og onlineredskaber for EU-procedurer (f.eks. det europæiske betalingspåkrav).

9. Den tilsynsførende støtter, at der sættes fokus på ovennævnte foranstaltninger. Han støtter generelt en samlet tilgang til e-justice. Han udtaler sin støtte til det tredobbelte behov for en bedre adgang til domstolene, et øget samarbejde mellem europæiske retsmyndigheder og en generel forbedring af retsvæsenets effektivitet. Som følge af denne tilgang berøres flere institutioner og personer:

   — Medlemsstaterne, som har hovedansvaret for, at der findes effektive og pålidelige retsvæsener.

   — Europa-Kommissionen i sin rolle som traktaternes vogter.

   — Medlemsstaternes retsmyndigheder, som har behov for mere avancerede kommunikationsredskaber, navnlig i grænseoverskridende sager.

   — De juridiske erhverv, borgerne og virksomhederne, som alle går ind for en mere udbredt brug af it-redskaber, så domstolene på en mere tilfredsstillende måde kan imødekomme deres behov.

10. Meddelelsen hænger tæt sammen med forslaget til Rådets afgørelse om indførelse af det europæiske informationssystem vedrørende strafferegistre (ECRIS). Den 16. september 2008 vedtog den tilsynsførende en udtalelse om dette forslag ([7]). Han støttede forslaget, under forudsætning af at der tages hensyn til en række overvejelser. Han påpegede navnlig, at yderligere databeskyttelsesgarantier bør kompensere for den nuværende mangel på en samlet retlig ramme vedrørende databeskyttelse på området samarbejde mellem politi og retsvæsen. Han fremhævede derfor behovet for effektiv koordination af databeskyttelsestilsyn med systemet, der involverer medlemsstaternes myndigheder og Kommissionen, som stiller den fælles kommunikationsinfrastruktur til rådighed.

11. Det er relevant at minde om følgende anbefalinger i denne udtalelse:

   — Det bør fremgå, at et højt databeskyttelsesniveau er en forudsætning for, at gennemførelsesforanstaltningerne kan vedtages.

   — Kommissionens ansvar for systemets fælles kommunikationsinfrastruktur samt anvendeligheden af forordning (EF) nr. 45/2001 bør præciseres for bedre at sikre retssikkerheden.

   — Kommissionen bør også være ansvarlig for sammenkoblingssoftwaren — og ikke medlemsstaterne — med henblik på at forbedre effektiviteten af udvekslingen og muliggøre et bedre tilsyn med systemet.

   — Anvendelse af maskinoversættelse bør klart defineres og afgrænses, således at den gensidige forståelse af strafbare handlinger kan fremmes, uden at det berører kvaliteten af de videregivne oplysninger.

12. Disse anbefalinger har fortsat gyldighed for den kontekst, hvori den foreliggende meddelelse vil blive analyseret.

III. DEN I MEDDELELSEN OMHANDLEDE UDVEKSLING AF OPLYSNINGER

13. E-justice har et meget bredt anvendelsesområde, herunder generelt anvendelsen af ikt i forbindelse med retspleje inden for Den Europæiske Union. Dette omfatter en række spørgsmål, som f.eks. projekter, der giver de retsundergivne oplysninger på en mere effektiv måde. Dette omfatter onlineoplysninger om retssystemer, lovgivning

([6]) Arbejdsdokument fra Kommissionens tjenestegrene — Ledsagedokument til meddelelsen til Rådet, Europa-Parlamentet og det Europæiske Økonomiske og Sociale Udvalg »På vej mod en EU-strategi for e-justice« — Resumé af konsekvensanalysen, SEK(2008)1944 af 30.5.2008.

([7]) Jf. den tilsynsførendes udtalelse om indførelse af det europæiske informationssystem vedrørende strafferegistre (ECRIS) i henhold til artikel 11 i rammeafgørelse 2008/XX/RIA, der er tilgængelig på den tilsynsførendes websted www.edps.europa.eu, »consultation« og derefter »opinions«, »2008«.

og retspraksis, elektroniske systemer for kommunikation mellem en sags parter og domstolene, og indførelse af fuldstændig elektroniske procedurer. Det omfatter også europæiske projekter, som f.eks. brug af elektroniske hjælpemidler til registrering af udtalelser på retsmøder, og projekter for udveksling af oplysninger eller sammenkobling af net.

14. Selv om anvendelsesområdet er meget bredt, har den tilsynsførende bemærket, at der vil være oplysninger om straffesager og om civil- og handelsretlige systemer men ikke om forvaltningsretlige systemer. Og der vil være et link til et strafferetligt og et civilretligt atlas men ikke til et atlas på forvaltningsområdet, selv om det måske ville være bedre for borgerne og virksomhederne at have adgang til retssystemerne på det administrative område, dvs. forvaltningsret og klageprocedurer. Der vil også blive etableret et link til Association of Councils of State. Disse tilføjelser ville kunne være en fordel for de borgere, der prøver at finde vej gennem den jungle — som forvaltningsretten med alle dens domstole ofte er — for således at blive bedre informeret om de forvaltningsretlige systemer.

15. Den tilsynsførende anbefaler derfor at medtage administrative procedurer i e-justice. Som en del af dette nye element bør der indledes e-justice-projekter for at gøre databeskyttelsesreglerne og de nationale databeskyttelsesmyndigheder mere synlige, navnlig i forbindelse med de typer oplysninger, der behandles inden for rammerne af e-justice. Dette ville være på linje med det såkaldte »London-initiativ«, som blev indledt af databeskyttelsesmyndighederne i november 2006, og som tager sigte på »Kommunikation om databeskyttelse og effektivisering heraf«.

IV **DEN NYE RAMMEAFGØRELSE OM BESKYTTELSE AF PERSONOPLYSNINGER I FORBINDELSE MED POLITISAMARBEJDE OG RETLIGT SAMARBEJDE I KRIMINALSAGER**

16. Som følge af den stigende udveksling af personoplysninger mellem retsmyndigheder, der er omhandlet i meddelelsen, antager de gældende retlige rammer for databeskyttelse en endnu større betydning. I den forbindelse noterer den tilsynsførende, at Rådet for Den Europæiske Union tre år efter Kommissionens oprindelige forslag vedtog rammeafgørelsen om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager den 27. november ([8]). Denne nye lovgivning vil fastlægge en generel ramme for databeskyttelse for så vidt angår spørgsmål under »tredje søjle« ud over databeskyttelsesbestemmelserne under »første søjle« i direktiv 95/46/EF.

17. Den tilsynsførende ser med tilfredshed på denne retsakt som det første væsentlige skridt fremad for databeskyttelse inden for politisamarbejde og retligt samarbejde. Det databeskyttelsesniveau, som man har nået frem til i den endelige tekst, er imidlertid ikke fuldt tilfredsstillende. Specielt omfatter rammeafgørelsen omfatter kun politimæssige og retlige oplysninger, der udveksles mellem medlemsstater, EU-myndigheder og -systemer, og omfatter ikke nationale oplysninger. Endvidere fastsættes der ikke i den vedtagne rammeafgørelse en forpligtelse til at sondre mellem forskellige kategorier af registrerede, såsom mistænkte, kriminelle, vidner og ofre, for at sikre, at deres oplysninger behandles med mere passende garantier. Den sikrer ikke fuld sammenhæng med direktiv 95/46/EF, navnlig for så vidt angår begrænsning af de formål, hvortil personoplysninger kan behandles yderligere. Den fastlægger heller ikke en uafhængig gruppe af relevante nationale og EU-databeskyttelsesmyndigheder, der ville kunne sikre både bedre koordination mellem databeskyttelsesmyndigheder og et betydeligt bidrag til en ensartet anvendelse af rammeafgørelsen.

18. Dette betyder, at der i en sammenhæng, hvor der er gjort en stor indsats for at udvikle fælles systemer for grænseoverskridende udveksling af personoplysninger, stadig eksisterer forskelle med hensyn til reglerne for behandling af disse oplysninger, og i overensstemmelse med hvilke borgerne kan udøve deres rettigheder i forskellige EU-lande.

19. Den tilsynsførende minder på ny om, at sikring af et højt databeskyttelsesniveau inden for politisamarbejde og retligt samarbejde samt overensstemmelse med direktiv 95/46/EF udgør et nødvendigt supplement til andre foranstaltninger, der er indført eller påtænkt for at lette grænseoverskridende udveksling af personoplysninger i forbindelse med retshåndhævelse. Dette skyldes ikke kun borgernes ret til, at de grundlæggende rettigheder til beskyttelse af personoplysninger overholdes, men også retshåndhævelsesmyndighedernes behov for at sikre kvaliteten af de udvekslede oplysninger — hvilket bekræftes i bilaget til meddelelsen for så vidt angår sammenkobling af strafferegistre — tillid mellem myndigheder i forskellige lande og endelig retsgyldigheden af det bevismateriale, der er indsamlet i en grænseoverskridende sammenhæng.

20. Derfor opfordrer den tilsynsførende EU-institutionerne til specifikt at tage hensyn til disse elementer, ikke kun ved gennemførelsen af de foranstaltninger, der er indeholdt i meddelelsen, men også med henblik på snarest muligt at indlede overvejelser om yderligere forbedringer af den retlige ramme for databeskyttelse i forbindelse med retshåndhævelse.

V. **E-JUSTICE-PROJEKTER**

E-justice-redskaber på EU-plan

21. Den tilsynsførende anerkender, at udveksling af personoplysninger er af afgørende betydning for etableringen af et område med frihed, sikkerhed og retfærdighed. Af den grund støtter den tilsynsførende forslaget til en strategi for e-justice, og fremhæver i denne forbindelse også betydningen af databeskyttelse. Overholdelse af databeskyttelse er ikke kun en retlig forpligtelse men også en vigtig faktor, hvis de påtænkte systemer skal blive en succes, f.eks. med hensyn til at sikre kvaliteten af dataudvekslingerne. Det gælder også for institutionerne og organerne, når de skal

([8]) Endnu ikke offentliggjort i Europæiske Unions Tidende.

behandle personoplysninger, og når der skal udformes nye politikker. Reglerne og principperne bør anvendes og følges i praksis og navnlig tages i betragtning ved udformningen og opbygningen af informationssystemer. Beskyttelse af privatlivets fred og databeskyttelse er i alt væsentligt »nøglefaktorer for succes« for et fremgangsrigt og velafbalanceret informationssamfund. Det giver derfor mening at investere i dem og at gøre dette så tidligt som muligt.

22. I den forbindelse understreger den tilsynsførende, at meddelelsen ikke omhandler en central europæisk database. Han hilser det velkommen, at man har foretrukket den decentraliserede arkitektur. Den tilsynsførende erindrer om, at han har afgivet udtalelse om ECRIS ([9]) og om Prüminitiativet ([10]). I udtalelsen om ECRIS gav den tilsynsførende udtryk for, at en decentraliseret arkitektur undgår yderligere dobbeltregistrering af personoplysninger i en central database. I udtalelsen om Prüm-initiativet anbefaler han, at der tages behørigt hensyn til størrelsen af systemet under drøftelserne om sammenkobling af databaser. Der bør navnlig indføres særlige formater for datakommunikation, som f.eks. anmodninger om strafferegistre, der foretages online, også under hensyntagen til sprogforskellene, og nøjagtigheden af dataudvekslingen bør konstant overvåges. Disse elementer bør også tages i betragtning i forbindelse med initiativer, der stammer fra strategien for e-justice.

23. Europa-Kommissionen agter i tæt samarbejde med medlemsstaterne og andre partnere at bidrage til en styrkelse og udvikling af e-justice-redskaber på EU-plan. Samtidig med at den vil støtte medlemsstaternes bestræbelser, har den til hensigt selv at udvikle et vist antal it-redskaber. De vil gøre det muligt at forbedre interoperabiliteten mellem systemerne, at lette borgernes adgang til retsvæsenet og forbedre kommunikationen mellem retsmyndighederne samt at opnå væsentlige stordriftsfordele på EU-plan. Med hensyn til interoperabilitet mellem den software, medlemsstaterne anvender, skal alle medlemsstater ikke nødvendigvis anvende samme software — selv om dette vil være den mest praktiske løsning — men softwaren skal være fuldt interoperabel.

24. Den tilsynsførende anbefaler, at sammenkoblingen og interoperabiliteten mellem systemerne tager behørigt hensyn til princippet om formålsbegrænsning og baseres på databeskyttelsesnormer (»indbygget databeskyttelse«). Enhver form for interaktion mellem forskellige systemer bør være grundigt dokumenteret. Interoperabilitet må aldrig føre til en situation, hvor en myndighed, der ikke har adgang til eller ikke har ret til at anvende visse oplysninger, kan opnå denne adgang via adgangen til et andet informationssystem. Den tilsynsførende ønsker på ny at understrege, at interoperabilitet i sig selv ikke bør berettige en omgåelse af princippet om formålsbegrænsning ([11]).

25. Et andet afgørende punkt er at sikre, at øget grænseoverskridende udveksling af personoplysninger ledsages af øget tilsyn og samarbejde fra databeskyttelsesmyndighedernes side. Den tilsynsførende har allerede i sin udtalelse af 29. maj 2006 om rammeafgørelsen om udveksling af strafferegistre ([12]) understreget, at den foreslåede rammeafgørelse ikke kun bør omhandle samarbejdet mellem de centrale myndigheder, men også samarbejdet mellem forskellige kompetente databeskyttelsesmyndigheder. Dette behov er blevet så meget desto vigtigere, som at forhandlingerne vedrørende den nyligt vedtagne rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager ([13]) førte til udeladelse af bestemmelsen om oprettelse af en arbejdsgruppe, der samler EU's databeskyttelsesmyndigheder og koordinerer deres aktiviteter med hensyn til behandling af oplysninger inden for rammerne af politisamarbejde og retligt samarbejde i kriminalsager. Med henblik på at sikre et effektivt tilsyn samt tilfredsstillende kvalitet af den grænseoverskridende cirkulation af oplysninger fra strafferegistre, bør der derfor indføres mekanismer for effektiv koordination mellem databeskyttelsesmyndigheder ([14]). Disse mekanismer bør også tage hensyn til den tilsynsførendes tilsynsbeføjelser med hensyn til S-TESTA-infrastrukturen ([15]). E-justice-redskaber vil kunne understøtte disse mekanismer, der vil kunne udvikles i tæt samarbejde med databeskyttelsesmyndighederne.

26. I punkt 4.2.1 i meddelelsen påpeges det , at det er vigtigt, at denne udveksling af oplysninger fra strafferegistre også udvides til at omfatte mere end det retslige samarbejde, således at der integreres andre formål, f.eks. adgang til at kunne få visse stillinger. Den tilsynsførende understreger, at enhver behandling af personoplysninger til andre formål end dem, hvortil de er indsamlet, skal overholde de specifikke betingelser i den gældende databeskyttelseslovgivning. Navnlig bør behandling af personoplysninger til yderligere formål kun tillades, hvis det er nødvendigt til at

([9]) Se fodnote 4, pkt. 18.
([10]) EUT C 89 af 10.4.2008, s. 4.
([11]) EUT C 91 af 19.4.2006, s. 53. Jf. også den tilsynsførendes bemærkninger til Kommissionens meddelelse om kompatibilitet mellem europæiske databaser, 10.3.2006, Bruxelles.
([12]) EUT C 313, 20.12.2006, s. 26.
([13]) Jf. ovenfor kapitel IV.
([14]) Jf. den tilsynsførende udtalelse om ECRIS, punkt 8 og 37-38.
([15]) Jf. i denne forbindelse punkt 27-28.

forfølge interesser som opført i Fællesskabets databeskyttelseslovgivning ([16]), og under forudsætning af, at de er fastsat i lovgivningsmæssige foranstaltninger.

27. I meddelelsen hedder det med hensyn til sammenkobling af strafferegistre, at Kommissionen som led i forberedelserne af ikrafttrædelsen af rammeafgørelsen om udveksling af oplysninger fra strafferegistre vil indlede to gennemførlighedsundersøgelser for at tilrettelægge projektet efterhånden som det skrider frem, og at udvide udvekslingen af oplysninger til at omfatte tredjelandsstatsborgere, der er dømt for strafbare handlinger. Kommissionen stiller i 2009 software, der er udformet, så det gør det muligt at udveksle alle strafferegistre hurtigt, til rådighed for medlemsstaterne. Dette referencesystem kombineret med anvendelsen af S-TESTA med henblik på udveksling af oplysninger vil give stordriftsfordele, da medlemsstaterne ikke vil skulle foretage deres eget udviklingsarbejde. Det vil også gøre det lettere at gennemføre projektet.

28. I den forbindelse hilser den tilsynsførende anvendelsen af S-TESTA-infrastrukturen, der har vist sig at være et pålideligt system for udveksling af data, velkommen, og anbefaler, at de statistiske elementer vedrørende de påtænkte dataudvekslingssystemer fastlægges i detaljer og tager behørigt hensyn til nødvendigheden af at sikre databeskyttelsestilsyn. Statistiske oplysninger kan f.eks. udtrykkelig omfatte elementer såsom antallet af anmodninger om adgang til eller rettelser af personoplysninger, længden og fuldstændigheden af opdateringsprocessen, krav vedrørende personer, der har adgang til disse oplysninger samt sager om sikkerhedsbrud. Desuden bør statistiske oplysninger og rapporter på grundlag af dem være fuldt tilgængelige for kompetente databeskyttelsesmyndigheder.

Maskinoversættelse og databasen for oversættere

29. Anvendelsen af maskinoversættelse er et nyttigt instrument og vil sandsynligvis fremme den gensidige forståelse mellem de relevante aktører i medlemsstaterne. Anvendelsen af maskinoversættelse bør dog ikke føre til en nedgang i kvaliteten af de oplysninger, der udveksles, navnlig når disse oplysninger benyttes til at træffe beslutninger, som har retsvirkninger for de berørte personer. Den tilsynsførende påpeger, at det er vigtigt klart at definere og afgrænse anvendelsen af maskinoversættelse. Anvendelsen af maskinoversættelse ved videregivelsen af oplysninger, der ikke er blevet korrekt præoversat, som f.eks. bemærkninger eller specifikationer, der er tilføjet i de enkelte sager, vil kunne påvirke kvaliteten af de videregivne oplysninger — og således af de afgørelser, der træffes på grundlag heraf — og bør i princippet udelukkes ([17]). Den tilsynsførende foreslår, at denne henstilling tages i betragtning i forbindelse med de foranstaltninger, der følger af meddelelsen.

30. Kommissionen ønsker at oprette en database over juridiske oversættere og tolke, således at kvaliteten af juridisk oversættelse og tolkning kan forbedres. Den tilsynsførende støtter dette mål, men minder om, at denne database vil afhænge af anvendelsen af de relevante databeskyttelsesbestemmelser. Navnlig hvis databasen skal indeholde evalueringsoplysninger om oversætternes præstationer, kan det kræve, at de kompetente databeskyttelsesmyndigheder foretager forudgående kontrol.

På vej mod en EU-strategi for e-justice

31. Det fremgår af punkt 5 i meddelelsen, at der skal fastlægges en klar kompetencefordeling mellem Kommissionen, medlemsstaterne og de øvrige aktører i det retslige samarbejde. Kommissionen vil tage sig af den overordnede koordinering og i den forbindelse fremme udvekslingen af god praksis og vil udforme, indføre og koordinere informationen om e-justice-portalen. Endvidere vil Kommissionen forsætte arbejdet med sammenkobling af strafferegistre og fortsat påtage sig det direkte ansvar for det civilretlige netværk og støtte det strafferetlige netværk. Medlemsstaterne skal ajourføre de oplysninger om deres retssystemer, som findes på e-justice-webstedet. Andre aktører er de civil- og strafferetlige netværk og Eurojust. De vil udvikle de redskaber, der er nødvendige for et mere effektivt retsligt samarbejde, navnlig automatiserede oversættelsesredskaber og sikre udvekslingssystemer, i nær kontakt med Kommissionen. Et udkast til handlingsplan og en tidsplan for de forskellige projekter er vedlagt meddelelsen.

32. I den forbindelse understreger den tilsynsførende, at der i ECRIS-systemet på den ene side ikke er oprettet nogen central europæisk database, og det er ikke meningen, at der skal etableres direkte adgang til databaser som dem, der indeholder andre medlemsstaters strafferegistre, mens ansvaret for korrekt information på nationalt plan på den anden side er samlet hos medlemsstaternes centrale myndigheder. Inden for rammerne af denne mekanisme har medlemsstaterne ansvaret for driften af de nationale databaser og for, at udvekslingen fungerer effektivt. Det er ikke klart, om de er ansvarlige for sammenkoblingssoftware eller ej. Kommissionen vil inden længe stille software, der er udformet, så det gør det muligt at udveksle alle strafferegistre, til rådighed for medlemsstaterne. Dette referencesystem vil blive kombineret med anvendelsen af S-TESTA med henblik på udveksling af oplysninger.

33. Den tilsynsførende formoder, at der også i forbindelse med tilsvarende e-justice-initiativer kan blive implementeret lignende systemer, og at Kommissionen vil være ansvarlig for den fælles infrastruktur, selv om det ikke fremgår af meddelelsen. Den tilsynsførende foreslår, at dette ansvar

([16]) Jf. især artikel 13 i direktiv 95/46/EF nr. og artikel 20 i forordning (EF) nr. 45/2001.

([17]) Se punkt 39-40 i den tilsynsførendes udtalelse om ECRIS.

kommer til at fremgå tydeligt af de foranstaltninger, der er afledt af meddelelsen, af hensyn til retssikkerheden.

E-justice-projekter

34. I bilaget er der anført en række projekter, som skal udvikles i løbet af de næste fem år. Det første projekt, udvikling af websider om e-justice, vedrører e-justice-portalen. Denne foranstaltning forudsætter en gennemførlighedsundersøgelse og udvikling af portalen. Endvidere kræver den implementering af forvaltningsmetoder og online-information på alle EU-sprog. Det andet og tredje projekt vedrører sammenkobling af strafferegistre. Det andet projekt vedrører sammenkobling af de nationale strafferegistre. Det tredje projekt vedrører oprettelse af en EU-fortegnelse over dømte tredjelandsstatsborgere i forlængelse af en gennemførlighedsundersøgelse og forelæggelse af et forslag til retsakt. Den tilsynsførende bemærker, at sidstnævnte projekt ikke længere er nævnt i Kommissionens arbejdsprogram, og er i tvivl om, hvorvidt dette afspejler en ændring i Kommissionens påtænkte projekter eller blot en udsættelse af dette specifikke projekt.

35. Meddelelsen anfører også tre projekter inden for elektronisk udveksling og tre projekter inden for hjælp til oversættelse. Der vil blive indledt et pilotprojekt om gradvis udarbejdelse af et flersproget juridisk vokabular. Andre relevante projekter vedrører indførelse af dynamiske formularer i forbindelse med EU's retsakter samt fremme af retsmyndighedernes brug af videokonferencer. Endelig vil der i forbindelse med e-justice-forummet blive holdt årlige møder om emneområdet e-justice og etableret uddannelse af jurister i det retslige samarbejde. Den tilsynsførende foreslår, at man i forbindelse med disse møder og uddannelser er tilstrækkelig opmærksom på lovgivningen og praksis vedrørende databeskyttelse.

36. I bilaget foreslås der derfor en bred vifte af europæiske værktøjer med henblik på at lette udvekslingen af oplysninger mellem aktører i forskellige medlemsstater. Blandt disse værktøjer vil e-justice-portalen, som Kommissionen bliver hovedansvarlig for, komme til at spille en vigtig rolle.

37. Et fælles træk ved mange af disse værktøjer bliver, at oplysninger, herunder personoplysninger, vil blive udvekslet og behandlet af mange forskellige aktører på såvel nationalt plan som EU-plan, der er underlagt databeskyttelsesforpligtelser og tilsynsmyndigheder, som følger af direktiv 95/46/EF eller forordning (EF) nr. 45/2001. I den forbindelse har den tilsynsførende allerede gjort det klart i sin udtalelse om informationssystemet for det indre marked (IMI) ([18]), at ansvaret for overholdelsen af databeskyttelseslove sikres på en effektiv og gnidningsløs måde.

38. Grundlæggende kræver dette på den ene side en klar afgrænsning og fordeling af ansvaret for behandlingen af personoplysninger inden for disse systemer og på den anden side, at der, når det er nødvendigt, indføres passende koordineringsmekanismer, navnlig for tilsyn.

39. Anvendelsen ny teknologi er en af hovedhjørnestenene i e-justice-initiativerne: sammenkobling af nationale registre, udvikling af elektronisk underskrift, sikre net, platforme for virtuel udveksling af oplysninger og øget brug af videokonferencer vil være vigtige elementer i e-justice-initiativerne i løbet af de kommende år.

40. Det er i den forbindelse vigtigt, at der tages hensyn til databeskyttelsesspørgsmål så tidligt som muligt, og at de forankres i de påtænkte værktøjers arkitektur. Både systemets arkitektur og implementeringen af relevante sikkerhedsforanstaltninger er særlig vigtige. Denne »indbyggede databeskyttelse« vil gøre det muligt for de relevante e-justice-initiativer at sikre effektiv forvaltning af personoplysninger og samtidig sikre overholdelse af databeskyttelsesprincipperne og sikkerhed i forbindelse med udveksling af oplysninger mellem forskellige myndigheder.

41. Endvidere fremhæver den tilsynsførende, at teknologiske værktøjer ikke kun bør anvendes til at sikre udveksling af oplysninger, men også til at forbedre de registrerede personers rettigheder. Ud fra dette perspektiv hilser den tilsynsførende det velkommen, at meddelelsen nævner, at borgerne skal have mulighed for online at anmode om en udskrift af deres straffeattest på det sprog, de måtte ønske ([19]). Med hensyn til dette spørgsmål minder den tilsynsførende om, at han i sin udtalelse om Kommissionens forslag om udveksling af strafferegistre så med tilfredshed på, at den registrerede kunne anmode den centrale myndighed i en medlemsstat om strafferegisteroplysninger om sig selv, forudsat at den registrerede er eller har været bosiddende eller statsborger i den anmodede eller anmodende medlemsstat. Tanken med at benytte den myndighed, der er tættest ved den registrerede, som »one-stop-shop«, blev også fremsat af den tilsynsførende i forbindelse med koordinering af sociale sikringsordninger.

([18]) EUT C 270 af 25.10.2008, s. 1.
([19]) Se s. 6 i meddelelsen.

Den tilsynsførende opfordrer derfor Kommissionen til at gå videre ad samme spor ved at fremme teknologiske værktøjer og navnlig onlineadgang, hvorved borgerne bliver bedre i stand til at kontrollere deres personoplysninger, selv når de flytter mellem forskellige medlemsstater.

VI. **KONKLUSIONER**

42. Den tilsynsførende støtter forslaget om oprettelse af e-justice og anbefaler, at bemærkningerne i denne udtalelse tages i betragtning; dette indebærer:

— at der tages hensyn til den seneste rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, herunder dens mangler, ikke blot ved gennemførelsen af de foranstaltninger, der overvejes i meddelelsen, men også med henblik på snarest muligt at indlede overvejelser om yderligere forbedringer af lovgivningen om databeskyttelse i forbindelser med retshåndhævelse

— at administrative procedurer medtages i e-justice. Som led i dette nye element bør der påbegyndes e-justice-projekter for at gøre databeskyttelsesreglerne samt de nationale databeskyttelsesmyndigheder mere synlige, navnlig i relation til de typer oplysninger, der behandles som led i e-justice-projekter

— at decentraliserede arkitekturer fortsat skal foretrækkes

— at det sikres, at sammenkoblingen og interoperabiliteten mellem systemerne tager behørigt hensyn til princippet om formålsbegrænsning

— at alle aktører, der behandler personoplysninger inden for de påtænkte systemer, tildeles klare ansvarsområder, og at der tilvejebringes mekanismer for effektiv koordinering mellem databeskyttelsesmyndighederne

— at det sikres, at behandling af personoplysninger til andre formål end dem, hvortil de er indsamlet, overholder de specifikke betingelser i den gældende databeskyttelseslovgivning

— at anvendelsen af maskinoversættelse defineres og afgrænses klart for at fremme gensidig forståelse af strafbare handlinger, uden dermed at forringe kvaliteten af de fremsendte oplysninger

— at Kommissionens ansvar for fælles infrastrukturer såsom S-TESTA præciseres

— at det med hensyn til anvendelse af nye teknologier sikres, at databeskyttelsesspørgsmål tages i betragtning så tidligt som muligt tages (»indbygget databeskyttelse«), samt at teknologiværktøjer, der gør det muligt for borgerne bedre at kontrollere deres personoplysninger, selv når de flytter mellem flere medlemsstater, fremmes.

Udfærdiget i Bruxelles, den 19. december 2008.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser

(2009/C 128/03)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser 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,

som henviser 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, særlig artikel 41, og

som henviser til anmodningen om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev sendt til den tilsynsførende den 2. juli 2008,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

Forslaget til direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser

1. Den 2. juli 2008 vedtog Kommissionen et forslag til Europa-Parlamentets og Rådets direktiv om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (i det følgende benævnt »forslaget«) ([1]). Forslaget blev af Kommissionen forelagt den tilsynsførende med henblik på en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001.

2. Forslaget tager sigte på fastlæggelse af en fællesskabsramme for levering af grænseoverskridende sundhedsydelser i EU i de tilfælde, hvor den behandling, som patienten ønsker, udføres i en anden medlemsstat end hjemlandet. Det er struktureret omkring tre hovedområder:

— fastlæggelse af fælles principper i alle EU's sundhedssystemer med tydelig angivelse af medlemsstaternes ansvar

— udarbejdelse af en særlig ramme for grænseoverskridende sundhedsydelser, der præciserer patienters rettigheder til at gøre brug af sundhedsydelser i andre medlemsstater

— fremme af EU-samarbejdet på områder som f.eks. anerkendelse af recepter udskrevet i andre lande, netværk af europæiske referencecentre, vurdering af sundhedsteknologi, dataindsamling, kvalitet og sikkerhed.

3. Denne ramme har et dobbelt formål: at skabe tilstrækkelig klarhed om retten til godtgørelse af udgifter til sundhedsydelser i andre medlemsstater og sikre, at de nødvendige krav med hensyn til sikre og effektive sundhedsydelser af høj kvalitet opfyldes, når der er tale om grænseoverskridende ydelser.

4. Gennemførelsen af en ordning for grænseoverskridende sundhedsydelser kræver udveksling af de relevante personoplysninger om helbredsforhold (i det følgende benævnt: »helbredsoplysninger«) om patienterne mellem godkendte organisationer og sundhedsprofessionelle i de forskellige medlemsstater. Disse oplysninger anses for at være følsomme og er omfattet af de strengere databeskyttelsesregler i artikel 8 i direktiv 95/46/EF om særlige kategorier af oplysninger.

Høring af den tilsynsførende

5. Den tilsynsførende hilser det velkommen, at han høres om dette spørgsmål, og at der henvises til denne høring i forslagets præambel, jf. artikel 28 i forordning (EF) nr. 45/2001.

6. Det er første gang, den tilsynsførende høres formelt om et forslag til direktiv om sundhedsydelser. Nogle af bemærkningerne i denne udtalelse er derfor af bredere karakter og vedrører almindelige spørgsmål angående beskyttelse af personoplysninger i sundhedssektoren, som også kan gælde for andre relevante (bindende eller ikke-bindende) retsakter.

([1]) KOM(2008) 414 endelig. Det bemærkes, at der samme dag blev vedtaget en supplerende meddelelse om en fællesskabsramme for patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (KOM(2008) 415 endelig). Eftersom meddelelsen er af ret generel karakter, har den tilsynsførende dog valgt at fokusere på direktivforslaget.

7. Den tilsynsførende ønsker allerede i starten at udtrykke sin støtte til initiativer, der tager sigte på at forbedre vilkårene for grænseoverskridende sundhedsydelser. Forslaget bør faktisk ses i kontekst af det overordnede EF-program til forbedring af borgernes sundhed i informationssamfundet. Andre initiativer i den forbindelse er Kommissionens planer om et direktiv og en meddelelse om donation af menneskelige organer og transplantation ([1]), henstillingen om interoperabilitet mellem elektroniske patientjournalsystemer ([2]) og den planlagte meddelelse om telemedicin ([3]). Den tilsynsførende er imidlertid betænkelig ved, at alle disse beslægtede initiativer ikke hænger tæt sammen og/eller er indbyrdes forbundet på området privatlivets fred og datasikkerhed og derfor er til hinder for vedtagelsen af en ensartet databeskyttelsestilgang på sundhedsområdet, især når det gælder brugen af nye ikt-teknologier. Til eksempel kan det nævnes, at selv om telemedicin nævnes udtrykkeligt i betragtning 10 i direktivforslaget, henvises der ikke til den relevante kommissionsmeddelelses databeskyttelsesdimension. Selv om elektroniske patientjournaler er en mulig metode til grænseoverskridende meddelelse af helbredsoplysninger, etableres der ikke nogen sammenhæng med de spørgsmål vedrørende privatlivets fred, der behandles i den relevante kommissionshenstilling ([4]). Dette giver indtryk af, at der stadig ikke er nogen klar definition af et overordnet perspektiv for privatlivets fred i forbindelse med sundhedsydelser, og at dette i nogle tilfælde helt mangler.

8. Dette er også tydeligt i det foreliggende forslag, hvor den tilsynsførende beklager at måtte konstatere, at der ikke tages konkret fat på databeskyttelseskonsekvenserne. Der er naturligvis henvisninger til databeskyttelse, men disse er hovedsagelig af generel karakter og afspejler ikke på en dækkende måde de specifikke behov og krav i relation til privatlivets fred i forbindelse grænseoverskridende sundhedsydelser.

9. Den tilsynsførende vil gerne understrege, at en ensartet og solid databeskyttelsestilgang, der dækker hele rækken af foreslåede instrumenter for sundhedsydelser, ikke blot vil sikre borgernes grundlæggende ret til beskyttelse af personoplysninger, men også vil bidrage til videreudvikling af grænseoverskridende sundhedsydelser i EU.

II. DATABESKYTTELSE I FORBINDELSE MED GRÆNSEOVERSKRIDENDE SUNDHEDSYDELSER

Generel baggrund

10. Det Europæiske Fællesskabs mest fremtrædende mål har været at etablere et indre marked og et område uden indre grænser, hvor den frie bevægelighed for varer, personer, tjenesteydelser og kapital er sikret. Det forhold, at borgerne har fået lettere ved at flytte til og bosætte sig i andre medlemsstater, har naturligvis givet anledning til spørgsmål vedrørende sundhedsydelser. Af den grund blev Domstolen tilbage i 1990'erne i forbindelse med det indre marked konfronteret med spørgsmål vedrørende eventuel refusion af lægeudgifter, som borgerne havde haft i andre medlemsstater. Domstolen anerkendte, at fri udveksling af tjenesteydelser som fastsat i EF-traktatens artikel 49 omfatter friheden for personer til at rejse til en anden medlemsstat for at modtage lægebehandling ([5]). Som følge heraf kunne patienter, som ønskede at modtage grænseoverskridende sundhedsydelser, ikke længere behandles anderledes end statsborgere i deres hjemland, som modtog samme lægebehandling uden at rejse over nogen grænser.

11. Disse domme er kernen i det foreliggende forslag. Eftersom Domstolens retspraksis er baseret på individuelle sager, er hensigten med det foreliggende forslag at øge klarheden for at sikre en mere generel og effektiv anvendelse af friheden til at modtage og levere sundhedsydelser. Men som allerede nævnt er forslaget også et led i et mere ambitiøst program, der har til formål at forbedre borgernes sundhed i informationssamfundet, hvor EU ser store muligheder for at fremme grænseoverskridende sundhedsydelser ved brug af informationsteknologi.

12. Af indlysende grunde er det et delikat spørgsmål at fastsætte regler for grænseoverskridende sundhedsydelser. Det berører et følsomt område, hvor medlemsstaterne har etableret forskellige nationale systemer, f.eks. med hensyn til forsikring og refusion af udgifter eller organisation af behandlingsinfrastrukturen, herunder net og applikationer for information om sundhedsydelser. Selv om fællesskabslovgiveren i det foreliggende forslag udelukkende koncentrerer sig om *grænseoverskridende* sundhedsydelser, vil reglerne i det mindste få indflydelse på, hvordan de nationale sundhedssektorer organiseres.

13. En forbedring af betingelserne for grænseoverskridende sundhedsydelser vil være til fordel for borgerne. Men en sådan forbedring vil samtidig også indebære visse risici for borgerne. Der skal findes en løsning på en lang række praktiske problemer, som kendetegner grænseoverskridende samarbejde mellem mennesker fra forskellige lande, der taler forskellige sprog. Eftersom et godt helbred er af allerstørste betydning for alle borgere, bør enhver risiko for fejlagtig kommunikation og efterfølgende unøjagtighed udelukkes. Det siger sig selv, at fremme af grænseoverskridende sundhedsydelser i kombination med udnyttelse af den informationsteknologiske udvikling har store konsekvenser for beskyttelsen af personoplysninger. En mere effektiv og derfor øget udveksling af helbredsoplysninger, den større afstand mellem de berørte personer

([1]) Bebudet i Kommissionens arbejdsprogram.
([2]) Kommissionens henstilling af 2. juli 2008 om grænseoverskridende interoperabilitet mellem elektroniske patientjournalsystemer (meddelt under nummer K(2008) 3282), EUT L 190 af 18.7.2008, s. 37.
([3]) Bebudet i Kommissionens arbejdsprogram.
([4]) Dette illustreres af, at der ikke er nogen omtale af privatlivets fred eller databeskyttelse i den i fodnote 1 nævnte meddelelse, der tager sigte på fastsættelse af en fællesskabsramme for patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser.
([5]) Jf. sag 158/96, *Kohll*, Sml. 1998, s. I-1931, præmis 34. Jf. bl.a. sag C-157/99, *Smits og Peerbooms*, Sml. 2001, s. I-5473, og sag C-385/99, *Müller-Fauré og Van Riet*, Sml. 2003, s. I-12403.

og organer samt de forskellige nationale love til gennemførelse af databeskyttelsesreglerne rejser spørgsmål om datasikkerhed og retssikkerhed.

Beskyttelse af helbredsoplysninger

14. Det skal understreges, at helbredsoplysninger betragtes som en særlig kategori af oplysninger, der kræver større beskyttelse. Den Europæiske Menneskerettighedsdomstol har for nylig udtalt følgende i relation til artikel 8 i den europæiske menneskerettighedskonvention: Beskyttelse af personoplysninger, herunder navnlig medicinske data, er af afgørende betydning for, at en person kan udøve sin ret til respekt for privatliv og familieliv som sikret ved artikel 8 i konventionen ([1]). Før der gås nærmere ind på de strengere regler for behandling af helbredsoplysninger i direktiv 95/46/EF, skal der knyttes nogle få bemærkninger til begrebet »helbredsoplysninger«.

15. Direktiv 95/46/EF indeholder ikke nogen udtrykkelig definition af helbredsoplysninger. Der anvendes i almindelighed en bred fortolkning, hvor helbredsoplysninger ofte defineres som »personoplysninger [med] en klar og tæt forbindelse til beskrivelsen af en persons helbredstilstand« ([2]). Helbredsoplysninger omfatter i den forbindelse normalt medicinske data (f.eks. lægehenvisninger og recepter, lægeundersøgelsesrapporter, laboratorieprøver, røntgenbilleder osv.) såvel som administrative og finansielle helbredsrelaterede oplysninger (f.eks. dokumenter om hospitalsindlæggelse, sygesikringsnummer, lægeaftaler, regninger for sundhedsydelser osv.). Det bemærkes, at begrebet »medicinske data« ([3]) også af og til bruges som synonym for helbredsoplysninger ligesom begrebet »sundhedsoplysninger« ([4]). I hele denne udtalelse bruges begrebet »helbredsoplysninger«.

16. ISO-standard 27799 indeholder en nyttig definition af »helbredsoplysninger«: enhver oplysning, der vedrører en persons fysiske eller mentale helbred eller behandling af personens helbred, og som kan omfatte: a) oplysninger om registreringen af personen med henblik på ydelse af sundhedsydelser b) oplysninger om betaling for eller berettigelse til sundhedsydelser for så vidt angår personen c) et nummer, symbol eller særligt mærke, der tildeles en person for entydigt at identificere personen i sundhedsanliggender d) enhver oplysning om personen, som indsamles i tilknytning til ydelsen af sundhedsydelser til personen e) oplysninger, der hidrører fra testning eller undersøgelse af en legemsdel eller kroppens bestanddele og f) identificering af en person (sundhedsprofessionel) som yder af sundhedsydelser til personen.

17. Den tilsynsførende går stærkt ind for at vedtage en specifik definition af begrebet »helbredsoplysninger« i forbindelse med det foreliggende forslag, der også kan bruges fremover i andre relevante fællesskabsretsakter (jf. del III nedenfor).

18. Artikel 8 i direktiv 95/46/EF indeholder regler for behandlingen af særlige kategorier af oplysninger. Disse regler er strengere end dem, der gælder for behandling af andre oplysninger, jf. artikel 7 i direktiv 95/46/EF. Dette fremgår allerede af artikel 8, stk. 1, hvori det udtrykkeligt hedder, at medlemsstaterne *forbyder* behandling af bl.a. oplysninger om helbredsforhold. De efterfølgende stykker i artiklen indeholder flere undtagelser fra dette forbud, men disse er snævrere end betingelserne for behandling af almindelige oplysninger i artikel 7. F.eks. gælder forbuddet ikke, hvis den registrerede *udtrykkeligt* har givet sit samtykke (artikel 8, stk. 2, litra a)), hvorimod det ifølge artikel 7, litra a), i samme direktiv kræves, at *der ikke hersker tvivl* om, at den registrerede har givet sit samtykke. Endvidere kan det i en medlemsstats lovgivning fastsættes, at forbud ikke kan hæves selv ved den registreredes samtykke. Artikel 8, stk. 3, vedrører udelukkende behandling af oplysninger om helbredsforhold. Ifølge dette stykke finder forbuddet i stk. 1 ikke anvendelse, hvis behandlingen af oplysningerne er nødvendig med henblik på forebyggende medicin, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester, og hvis behandlingen af disse oplysninger foretages af en sundhedsprofessionel, der i henhold til den nationale lovgivning eller til regler, der er fastsat af kompetente nationale organer, har tavshedspligt, eller af en anden person med tilsvarende tavshedspligt.

19. Artikel 8 i direktiv 95/46/EF lægger stor vægt på, at medlemsstaterne bør sørge for tilstrækkelige eller fornødne garantier. Artikel 8, stk. 4, tillader f.eks. medlemsstaterne at fastsætte andre undtagelser fra forbuddet mod behandling af følsomme oplysninger af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, men med forbehold af, at der gives tilstrækkelige garantier. Dette understreger i generelle vendinger, at det er op til medlemsstaterne at være særlig omhyggelige, når det gælder behandling af følsomme oplysninger såsom helbredsoplysninger.

Beskyttelse af helbredsoplysninger i grænseoverskridende situationer

Delt ansvar mellem medlemsstaterne

20. Medlemsstaterne bør være særlig bevidste om dette ansvar, når der er tale om grænseoverskridende udveksling af helbredsoplysninger. Som nævnt ovenfor øger grænseoverskridende udveksling af helbredsoplysninger risikoen for unøjagtig eller ulovlig databehandling. Det siger sig selv, at dette kan få meget store negative følger for den registrerede. Både forsikringsmedlemsstaten (hvori patienten er

([1]) Jf. ECHR's dom af 17. juli 2008, *I mod Finland* (klage nr. 20511/03), præmis 38.

([2]) Jf. Artikel 29-Gruppen, Arbejdsdokument vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ), februar 2007, WP 131, punkt II.2. Jf. også den brede betydning af »personoplysninger«: Artikel 29-Gruppen, udtalelse 4/2007 om begrebet personoplysninger, WP 136.

([3]) Europarådets rekommandation nr. R(97)5 om beskyttelse af medicinske data.

([4]) ISO 27799:2008 »Sundhedsinformatik — Ledelsessystemer for informationssikkerhed i sundhedssektoren ved anvendelse af ISO/IEC 27002«.

forsikret) og behandlingsmedlemsstaten (på hvis område de grænseoverskridende sundhedsydelser faktisk udøves) er involveret i denne proces og deler derfor dette ansvar.

21. Helbredsoplysningers sikkerhed er i den forbindelse et vigtigt spørgsmål. I den nylige sag, der er nævnt ovenfor, lagde Den Europæiske Menneskerettighedsdomstol særlig vægt på helbredsoplysningernes fortrolighed: Respekten for helbredsoplysningernes fortrolighed er et afgørende princip i retssystemerne i alle konventionens kontraherende parter. Det er afgørende ikke blot at respektere en patients følelse af privatliv, men også at bevare hans eller hendes tillid til lægestanden og til sundhedstjenester i almindelighed ([1]).

22. Databeskyttelsesreglerne i direktiv 95/46/EF kræver endvidere, at forsikringsmedlemsstaten skal give patienten tilstrækkelig, korrekt og ajourført information om videregivelsen af hans eller hendes personoplysninger til en anden medlemsstat og samtidig sørge for en sikker videregivelse af oplysningerne til denne medlemsstat. Behandlingsmedlemsstaten bør også sørge for sikker modtagelse af disse oplysninger og for et passende beskyttelsesniveau, når oplysningerne faktisk behandles, jf. dens nationale databeskyttelseslovgivning.

23. Den tilsynsførende vil gerne gøre medlemsstaternes delte ansvar klart i forslaget, idet der også skal tages hensyn til elektronisk datakommunikation, især i forbindelse med nye ikt-applikationer, jf. nedenfor.

Elektronisk kommunikation af helbredsoplysninger

24. Den grænseoverskridende udveksling af helbredsoplysninger skal først og fremmest forbedres ved hjælp af informationsteknologi. Selv om der stadig kan foregå udveksling af oplysninger på papir under en ordning med grænseoverskridende sundhedsydelser (f.eks. hvis patienten flytter til en anden medlemsstat og tager alle sine relevante helbredsoplysninger med sig, såsom laboratorieprøver og lægehenvisninger), er det klart hensigten i stedet at bruge elektroniske medier. Den elektroniske kommunikation af helbredsoplysninger vil blive understøttet af de sundhedsinformationssystemer, der er etableret (eller skal etableres) i medlemsstaterne (på hospitaler, klinikker osv.), samt af ny teknologi såsom elektroniske patientjournalapplikationer (evt. ved brug af internettet) og andre redskaber som patient- og lægedatakort. Det er naturligvis også muligt at bruge en kombination af papirbaserede og elektroniske udvekslingsformer, afhængigt af medlemsstaternes sundhedssystemer.

25. E-sundheds- og telemedicinapplikationer, der er omfattet af direktivforslaget, vil blive helt afhængige af udveksling af elektroniske helbredsoplysninger (f.eks. livstegn, billeder osv.), normalt sammen med andre eksisterende elektroniske sundhedsinformationssystemer i behandlings- og forsikringsmedlemsstaterne. Dette omfatter også systemer, der virker både på patient-til-læge-basis (f.eks. fjernovervågning og -diagnose) og på læge-til-læge-basis (f.eks. fjernkonsultation mellem sundhedsprofessionelle for at indhente ekspertrådgivning om specifikke behandlingstilfælde). Andre mere specifikke sundhedsapplikationer, der støtter de overordnede grænseoverskridende sundhedsydelser, kan også være helt afhængige af elektronisk udveksling af oplysninger, f.eks. elektroniske recepter (e-recept) eller elektroniske henvisninger (e-henvisning), som allerede er indført i nogle medlemsstater ([2]).

Områder, der giver anledning til betænkeligheder, i forbindelse med grænseoverskridende udveksling af helbredsoplysninger

26. På baggrund af ovenstående betragtninger, medlemsstaternes sundhedssystemers forskellige opbygning og den tiltagende udvikling af e-sundheds-applikationer trænger følgende to hovedområder, der giver anledning til betænkeligheder, sig på for så vidt angår beskyttelse af personoplysninger i de grænseoverskridende sundhedsydelser: a) de forskellige sikkerhedsniveauer, som medlemsstaterne opererer med for beskyttelse af personoplysninger (tekniske og organisatoriske foranstaltninger), og b) integrering af beskyttelse af privatlivets fred i e-sundheds-applikationerne, ikke mindst i de nye tiltag, der udvikles. Desuden vil der også kunne være behov for at se nærmere på andre aspekter, såsom sekundær udnyttelse af helbredsoplysninger, specielt med henblik på udarbejdelse af statistikker. Disse spørgsmål analyseres mere indgående i resten af denne del.

Datasikkerheden i medlemsstaterne

27. Selv om direktiv 95/46/EF og direktiv 2002/58/EF anvendes ens i hele EU, kan der være forskel på, hvordan visse elementer tolkes og gennemføres fra land til land, navnlig på områder, hvor retsforskrifterne er generelt formulerede og overlades til medlemsstaterne. Et af de vigtigste områder, der giver anledning til betænkeligheder, er således behandlingssikkerheden, dvs. de (tekniske og organisatoriske) foranstaltninger, som medlemsstaterne træffer til at garantere helbredsoplysningernes sikkerhed.

([1]) Jf. ECHR's dom af 17. juli 2008, *I mod Finland* (klage nr. 20511/03), præmis 38.

([2]) eHealth ERA Report, Towards the Establishment of a European eHealth Research Area, Europa-Kommissionen, Informationssamfundet og Medier, marts 2007 http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Selv om den strenge beskyttelse af helbredsoplysninger er alle medlemsstaternes ansvar, findes der ikke i øjeblikket nogen almindeligt accepteret definition af et »passende« sikkerhedsniveau for sundhedsydelser i EU, som kunne anvendes, når der er tale om grænseoverskridende sundhedsydelser. Nationalt fastsatte databeskyttelsesregler vil f.eks. kunne pålægge et hospital i en medlemsstat at træffe bestemte sikkerhedsforanstaltninger (som f.eks. definition af en sikkerhedspolitik og adfærdskodekser, særlige regler for outsourcing og brug af eksterne kontrahenter, revisionskrav osv.), medens dette måske ikke er tilfældet i andre medlemsstater. Denne manglende harmonisering vil kunne få konsekvenser for den grænseoverskridende udveksling af oplysninger, navnlig i elektronisk form, eftersom det ikke kan garanteres, at oplysningerne (ud fra et teknisk og organisatorisk synspunkt) er sikret lige godt i de forskellige medlemsstater.

29. Der er derfor behov for yderligere harmonisering på dette område ved, at der defineres et fælles sæt sikkerhedskrav for sundhedsydelser, som alle medlemsstaternes sundhedstjenesteydere bør indføre. Dette behov er helt klart på linje med det overordnede behov for at fastlægge fælles principper i EU's sundhedssystemer, som er omhandlet i forslaget.

30. Dette bør ske generisk, uden at påtvinge medlemsstaterne bestemte tekniske løsninger, men med fastlæggelse af et grundlag for gensidig anerkendelse og accept, f.eks. vedrørende udformning af en sikkerhedspolitik, identificering og autentifikation af patienter og sundhedsprofessionelle osv. De eksisterende europæiske og internationale standarder (f.eks. ISO og CEN) for sundhedsydelser og sikkerhed, samt almindeligt accepterede og juridisk funderede tekniske begreber (som f.eks. elektronisk signatur [1]) vil kunne benyttes som køreplan for disse bestræbelser.

31. Den tilsynsførende støtter tanken om en harmonisering af sundhedsydelsessikkerheden på EU-plan og finder, at Kommissionen bør tage initiativer på dette område allerede inden for rammerne af det foreliggende forslag (jf. del III nedenfor).

Privatlivets fred i e-sundheds-applikationerne

32. Privatlivets fred og sikkerhedsaspekterne bør indgå i udformningen og gennemførelsen af ethvert sundhedssystem, navnlig e-sundheds-applikationer som omhandlet i dette forslag (»indbygget databeskyttelse«). Dette uomgængelige krav er tidligere blevet bakket op i andre relevante politikdokumenter [2], som både kan være af generel karakter og sundhedssektorspecifikke [3].

33. Inden for rammerne af den e-sundheds-interoperabilitet, der omhandles i forslaget, bør begrebet »indbygget databeskyttelse« endnu en gang fremhæves som et grundlag for alle de påtænkte udviklinger. Dette begreb finder anvendelse på flere forskellige niveauer: det organisatoriske, det semantiske og det tekniske niveau.

— På det organisatoriske niveau bør der tages hensyn til privatlivets fred ved udformningen af de nødvendige procedurer for udveksling af sundhedsoplysninger mellem medlemsstaternes sundhedsorganisationer. Dette vil kunne få direkte konsekvenser for udvekslingens karakter og også for, hvilke data der overføres (f.eks. brug af identifikationsnumre i stedet for patienternes rigtige navne, når dette er muligt).

— På det semantiske niveau bør kravene til privatlivets fred og sikkerheden indbygges i nye standarder og ordninger, f.eks. i udformningen af e-receptmodellen, som der også tales om i forslaget. Dette kunne baseres på de eksisterende standarder på området, f.eks. standarder for oplysningernes fortrolighed og digital signatur, og tackle sundhedssektorspecifikke behov som rollebaseret autentifikation af kvalificerede sundhedsprofessionelle.

— På det tekniske niveau bør systemarkitekturer og brugerapplikationer omfatte teknologier til sikring af privatlivets fred, som kan indføre ovennævnte semantiske definition.

34. Den tilsynsførende føler, at området elektroniske recepter kunne tjene som starten på integreringen af krav vedrørende privatlivets fred og sikkerheden på et meget tidligt udviklingstrin (jf. del III nedenfor).

Andre aspekter

35. Et andet aspekt, der også kunne inddrages i forbindelse med grænseoverskridende udveksling af helbredsoplysninger, er den sekundære udnyttelse af helbredsoplysninger og navnlig udnyttelse af oplysningerne til statistiske formål, som allerede er omhandlet i det foreliggende forslag.

36. Som nævnt i punkt 18 åbner artikel 8, stk. 4, i direktiv 95/46/EF mulighed for sekundær udnyttelse af helbredsoplysninger. Denne yderligere behandling bør dog kun ske af grunde, der vedrører hensynet til »vigtige samfundsmæssige interesser« og skal være omgærdet med »tilstrækkelige garantier«, der er fastsat i den nationale lovgivning eller efter afgørelse truffet af tilsynsmyndigheden [4]. I tilfælde af statistisk behandling af oplysninger opstår der endvidere, som nævnt i den tilsynsførendes udtalelse om forslaget til

[1] Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12-20).

[2] The EDPS and EU Research and Technological Development, Policy Paper, EDPS, April 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

[3] Kommissionens henstilling af 2. juli 2008 om grænseoverskridende interoperabilitet mellem elektroniske patientjournalsystemer (meddelt under nummer K(2008) 3282), EUT L 190 af 18.7.2008, s. 37.

[4] Jf. endvidere betragtning 34 i direktiv 95/46/EF. Med hensyn til dette punkt henvises der også til Artikel 29-Gruppens udtalelse om EPJ i fodnote 8 ovenfor.

forordning om fællesskabsstatistikker over folkesundhed og arbejdsmiljø ([1]), en øget risiko som følge af de forskellige betydninger, begreberne »fortrolighed« og »databeskyttelse« kan have i anvendelsen af databeskyttelseslovgivningen på den ene side og lovgivningen om statistikker på den anden side.

37. Den tilsynsførende ønsker at fremhæve ovennævnte elementer i forbindelse med det foreliggende forslag. Der bør henvises mere eksplicit til databeskyttelseskravene vedrørende den sekundære udnyttelse af helbredsoplysninger (jf. del III nedenfor).

III. DETALJERET ANALYSE AF FORSLAGET

Forslagets bestemmelser om databeskyttelse

38. Forslaget indeholder en række henvisninger til databeskyttelse og privatlivets fred i forskellige dele af dokumentet, herunder specielt:

— Det hedder bl.a. i betragtning 3, at direktivet skal gennemføres og anvendes under behørig hensyntagen til respekten for privatliv og beskyttelse af personoplysninger

— I betragtning 11 henvises der til den grundlæggende ret til privatlivets fred hvad angår behandling af personoplysninger og tavshedspligt som to af de operative principper, der er fælles for sundhedssystemerne i hele Fællesskabet.

— Betragtning 17 beskriver retten til beskyttelse af personoplysninger som en grundlæggende rettighed, som personer har, og som skal beskyttes, med særligt fokus på personers ret til indsigt i oplysninger om deres helbredsforhold — også i forbindelse med grænseoverskridende sundhedsydelser — som fastsat i direktiv 95/46/EF.

— I artikel 3, der fastsætter direktivets sammenhæng med andre fællesskabsbestemmelser, henvises der i stk. 1, litra a), til direktiv 95/46/EF og direktiv 2002/58/EF.

— I artikel 5 om behandlingsmedlemsstatens ansvar peges der i stk. 1, litra f), på beskyttelse af privatlivets fred som et af disse ansvarsområder i overensstemmelse med de nationale foranstaltninger til gennemførelse af direktiv 95/46/EF og direktiv 2002/58/EF.

— I artikel 6 om sundhedsydelser udført i en anden medlemsstat understreges det i stk. 5, at patienter, der tager til en anden medlemsstat for at gøre brug af sundhedsydelser der, eller som ønsker at gøre brug af sundhedsydelser i en anden medlemsstat, sikres adgang til deres journaler, igen i overensstemmelse med de nationale foranstaltninger til gennemførelse af direktiv 95/46/EF og direktiv 2002/58/EF.

— I artikel 12 om det nationale kontaktpunkt for grænseoverskridende sundhedsydelser hedder det i stk. 2, litra a), at disse kontaktpunkter bl.a. skal stille oplysninger til rådighed for patienterne om de garantier for beskyttelse af personoplysninger, der gives i en anden medlemsstat.

— I artikel 16 om e-sundhed hedder det, at de foranstaltninger, der er nødvendige for at opnå interoperabilitet i ikt-systemer, skal respektere den grundlæggende ret til beskyttelse af personoplysninger i overensstemmelse med den gældende lovgivning.

— Og endelig nævnes det bl.a. i artikel 18, stk. 1, at indsamlingen af data til statistikker og overvågningsformål skal ske i overensstemmelse med den nationale lovgivning og fællesskabslovgivningen om beskyttelse af personoplysninger.

39. Den tilsynsførende udtrykker tilfredshed med, at der er taget hensyn til databeskyttelsen under udarbejdelsen af forslaget, og at man har forsøgt at påpege det generelle behov for privatlivets fred i forbindelse med grænseoverskridende sundhedspleje. Men forslagets nuværende bestemmelser om databeskyttelse er enten for generelle eller henviser til medlemsstaternes ansvar på en ret selektiv og punktuel måde:

— Specielt vedrører betragtning 3 og 11 og artikel 3, stk. 1, litra a), artikel 16 og artikel 18, stk. 1, rent faktisk den overordnede retlige ramme for databeskyttelse (de to sidste for så vidt angår e-sundhed og indsamling af statistiske data, men uden at opstille specifikke krav vedrørende privatlivets fred).

— For så vidt angår medlemsstaternes ansvar er der en generel henvisning i artikel 5, stk. 1, litra f).

— Betragtning 17 og artikel 6, stk. 5, giver en mere specifik henvisning til patienternes ret til indsigt i behandlingsmedlemsstaten.

— Endelig indeholder artikel 12, stk. 2, litra a), en bestemmelse om patienternes ret til information i forsikringsmedlemsstaten (via de nationale kontaktpunkters indsats).

Som nævnt i indledningen til denne udtalelse er der desuden ikke nogen forbindelse og/eller henvisning til aspekter vedrørende privatlivets fred som omhandlet i andre (bindende eller ikke-bindende) EF-retsakter på sundhedsydelsesområdet, navnlig med hensyn til anvendelsen af nye ikt-applikationer (såsom telemedicin eller elektroniske journalsystemer).

([1]) EUT C 295 af 7.12.2007, s. 1.

40. Selv om privatlivets fred generelt er opstillet som et krav i forbindelse med grænseoverskridende sundhedsydelser, er det generelle billede således endnu ikke fuldstændigt, hverken for så vidt angår medlemsstaternes forpligtelser eller de særlige regler, der er indført i og med sundhedsydelsernes grænseoverskridende karakter (i modsætning til udbuddet af nationale sundhedsydelser). Mere specifikt skal følgende nævnes:

— Medlemsstaternes ansvar er ikke præsenteret på en integreret måde, eftersom visse forpligtelser (ret til indsigt og information) er fremhævet — i forskellige dele af forslaget — medens andre helt er udeladt, som f.eks. behandlingssikkerheden.

— Betænkelighederne ved medlemsstaternes uensartede sikkerhedsforanstaltninger og behovet for harmonisering af sikkerheden omkring helbredsoplysninger på europæisk plan i forbindelse med grænseoverskridende sundhedsydelser er ikke nævnt.

— Integreringen af privatlivets fred i e-sundheds-applikationerne er ikke nævnt. Det fremgår heller ikke tilstrækkelig tydeligt i forbindelse med e-recepter.

41. Desuden giver artikel 18, der vedrører indsamling af data til statistisk brug og overvågningsformål, anledning til visse betænkeligheder. I stk. 1 tales der om »statistiske og *andre supplerende data*«; der tales endvidere om »overvågningsformål« i flertal, og det er anført, hvilke områder der er omfattet af disse overvågningsformål, nemlig grænseoverskridende sundhedsydelser, de udførte ydelser, sundhedstjenesteyderne og patienterne, udgifterne og resultaterne. I denne kontekst, der allerede er ret uklar, følger en generel henvisning til databeskyttelseslovgivningen, men der opstilles ingen specifikke krav vedrørende den senere brug af helbredsoplysningerne, jf. artikel 8, stk. 4, i direktiv 95/46/EF. Endvidere indeholder stk. 2 en ubetinget forpligtelse til at indsende de mange data til Kommissionen mindst én gang om året. Da der ikke er nogen eksplicit henvisning til en vurdering af nødvendigheden af denne overførsel, ser det ud, som om fællesskabslovgiveren selv allerede har fastslået nødvendigheden af disse overførsler til Kommissionen.

Den tilsynsførendes henstillinger

42. Med henblik på at tackle ovennævnte aspekter på passende vis, fremsætter den tilsynsførende en række henstillinger i form af fem grundlæggende etaper for ændringer, som beskrevet i det følgende.

1.etape — Definition af helbredsoplysninger

43. Artikel 4 indeholder definitioner af de grundbegreber, der benyttes i forslaget. Den tilsynsførende henstiller, at der indsættes en definition af helbredsoplysninger i denne artikel. Der bør anlægges en bred fortolkning af helbredsoplysninger som den, der er beskrevet i del II i denne udtalelse (punkt 14 og 15).

2.etape — Indsættelse af en specifik artikel om databeskyttelse

44. Den tilsynsførende henstiller også kraftigt, at der i forslaget indsættes en specifik artikel om databeskyttelse, som kunne omhandle hele dimensionen vedrørende privatlivets fred på en klar og forståelig måde. Artiklen bør a) beskrive forsikringsmedlemsstatens og behandlingsmedlemsstatens ansvarsområder, herunder bl.a. behovet for sikkerhed i behandlingen, og b) udstikke de vigtigste områder for den videre udvikling, dvs. harmonisering af sikkerhedsbestemmelserne og integration af privatlivets fred i e-sundhed. Der kan medtages særlige bestemmelser om disse spørgsmål (i den foreslåede artikel), som beskrevet under etape 3 og 4.

3.etape — Særlig bestemmelse om harmonisering af sikkerhedsbestemmelserne

45. I forlængelse af ændringen i 2. etape henstiller den tilsynsførende, at Kommissionen vedtager en mekanisme til definition af et generelt accepteret sikkerhedsniveau for helbredsoplysninger på nationalt plan, idet der tages hensyn til de eksisterende tekniske standarder på området. Dette bør være afspejlet i forslaget. Gennemførelsen kan f.eks. ske efter udvalgsproceduren, som er defineret i artikel 19, og som gælder for andre dele af forslaget. Der kunne desuden også benyttes andre instrumenter til udarbejdelse af relevante retningslinjer, med inddragelse af alle berørte interessenter såsom Artikel 29-Udvalget og den tilsynsførende.

4.etape — Integration af privatlivets fred i e-recept-modellen

46. Artikel 14 om anerkendelse af recepter udstedt i en anden medlemsstat omhandler udvikling af en fællesskabsmodel for recepter med henblik på at sikre interoperabiliteten af e-recepter. Denne foranstaltning skal vedtages efter udvalgsproceduren som defineret i artikel 19, stk. 2, i forslaget.

47. Den tilsynsførende henstiller, at den foreslåede e-receptmodel medtager aspekterne privatlivets fred og sikkerhed, selv i den meget elementære semantiske definition af denne model. Dette bør udtrykkeligt anføres i artikel 14, stk. 2. litra a). Også her er det meget vigtigt at inddrage alle de relevante interessenter. Med hensyn til dette ønsker den tilsynsførende at blive holdt underrettet og inddraget i yderligere tiltag på dette område via den foreslåede udvalgsprocedure.

5.etape — Efterfølgende udnyttelse af helbredsoplysninger til statistiske formål og overvågningsformål

48. For at forebygge misforståelser opfordrer den tilsynsførende til at tydeliggøre begrebet »andre supplerende data« i artikel 18, stk. 1. Artiklen bør desuden ændres, så den mere specifikt henviser til kravene vedrørende efterfølgende udnyttelse af helbredsoplysninger som fastsat i artikel 8, stk. 4, i direktiv 95/46/EF. Desuden bør forpligtelsen i stk. 2 til at indsende alle oplysningerne til Kommissionen gøres betinget af en vurdering af nødvendigheden af sådanne overførsler til legitime formål, som er behørigt præciseret på forhånd.

IV. **KONKLUSIONER**

49. Den tilsynsførende ønsker at udtrykke sin støtte til initiativer, der tager sigte på at forbedre vilkårene for grænseoverskridende sundhedsydelser. Han udtrykker imidlertid betænkelighed ved det forhold, at fællesskabsinitiativer vedrørende sundhedsydelser ikke altid er ordentligt koordineret med hensyn til anvendelsen af ikt, privatlivets fred og sikkerheden, hvilket gør det vanskeligere at få fastlagt en alment gældende databeskyttelsesstrategi på sundhedsydelsesområdet.

50. Den tilsynsførende udtrykker tilfredshed med, at der er henvist til privatlivets fred i det foreliggende forslag. Det er dog som forklaret i del III i denne udtalelse nødvendigt at foretage en række ændringer, dels for at tydeliggøre kravene både for behandlings- og forsikringsmedlemsstaterne, dels for at tackle databeskyttelsesdimensionen af de grænseoverskridende sundhedsydelser korrekt:

— Der bør i artikel 4 indsættes en definition af helbredsoplysninger, som dækker alle personoplysninger med en klar og tæt forbindelse til beskrivelsen af en persons helbredstilstand. Dette bør i princippet også omfatte medicinske data og administrative og finansielle sundhedsrelaterede oplysninger.

— Det anbefales kraftigt at indsætte en specifik artikel om databeskyttelse. Denne artikel bør give et klart overblik og beskrive forsikringsmedlemsstatens og behandlingsmedlemsstatens ansvarsområder og udstikke de vigtigste områder for den videre udvikling, dvs. harmonisering af sikkerhedsbestemmelserne og integration af privatlivets fred, specielt i e-sundheds-applikationerne.

— Det henstilles, at Kommissionen inden for forslagets rammer indfører en mekanisme til definition af et generelt accepteret sikkerhedsniveau for helbredsoplysninger på nationalt plan, idet der tages hensyn til de eksisterende tekniske standarder på området. Der bør også tilskyndes til supplerende og/eller komplementære initiativer, der inddrager alle berørte interessenter, Artikel 29-Udvalget og den tilsynsførende.

— Det henstilles, at begrebet »indbygget databeskyttelse« indarbejdes i den foreslåede fællesskabsmodel for e-recepter (også på det semantiske plan). Dette bør udtrykkelig anføres i artikel 14, stk. 2. litra a). Den tilsynsførende ønsker at blive holdt underrettet og inddraget i yderligere tiltag på dette område via den foreslåede udvalgsprocedure.

— Det henstilles at præcisere affattelsen af artikel 18 og at indsætte en mere eksplicit henvisning til de specifikke krav vedrørende efterfølgende udnyttelse af helbredsoplysninger, jf. artikel 8, stk. 4, i direktiv 95/46/EF.

Udfærdiget i Bruxelles, den 2. december 2008.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

Anden udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om revisionen af direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation)

(2009/C 128/04)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser 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,

som henviser 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,

som henviser 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, særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

Baggrund

1. Europa-Kommissionen vedtog den 13. november 2007 et forslag om ændring af bl.a. direktivet om databeskyttelse inden for elektronisk kommunikation, sædvanligvis kaldet »e-databeskyttelsesdirektivet« ([1]) (i det følgende benævnt »forslaget« eller »Kommissionens forslag«). EDPS vedtog den 10. april 2008 en udtalelse om Kommissionens forslag, hvori han forelagde en række anbefalinger til forbedring af forslaget i et forsøg på at bidrage til at sikre, at de foreslåede ændringer fører til den bedst mulige beskyttelse af privatlivets fred og personoplysninger (»EDPS' første udtalelse«) ([2]).

2. EDPS hilste Kommissionens forslag om oprettelse af et obligatorisk system for underretning om brud på datasikkerheden velkommen; forslaget betyder, at virksomheder vil skulle underrette enkeltpersoner om, at deres personoplysninger er blevet lækket. Endvidere var han tilfreds med den nye bestemmelse, der giver juridiske personer (f.eks. forbrugerorganisationer og udbydere af internettjenester) mulighed for at anlægge sag mod spammere som supplement til de eksisterende redskaber til bekæmpelse af spam.

3. Under de drøftelser i Parlamentet, der gik forud for Europa-Parlamentets førstebehandling, gav EDPS yderligere råd, idet han fremkom med en række bemærkninger til udvalgte spørgsmål, der er rejst i betænkningerne fra de af Europa-Parlamentets udvalg, der er kompetente i forbindelse med revisionen af direktiverne om forsyningspligt ([3]) og e-databeskyttelse (»bemærkninger«) ([4]). Bemærkningerne omhandlede først og fremmest spørgsmål vedrørende behandling af trafikdata og beskyttelse af intellektuelle ejendomsrettigheder.

4. Europa-Parlamentet (»EP«) vedtog den 24. september 2008 en lovgivningsmæssig beslutning vedrørende e-databeskyttelsesdirektivet (»førstebehandlingsteksten«) ([5]). EDPS så positivt på flere af EP's ændringer, der blev vedtaget i forlængelse af ovennævnte udtalelse og bemærkninger fra EDPS. Blandt de vigtige ændringer var, at også udbydere af informationssamfundstjenester (dvs. virksomheder, der opererer på internettet) omfattes af forpligtelsen til at underrette om sikkerhedsbrud. EDPS udtrykte ligeledes tilfredshed med den ændring, der giver juridiske og fysiske personer mulighed for at anlægge sag ved overtrædelse af alle bestemmelserne i e-databeskyttelsesdirektivet velkommen (og ikke kun ved overtrædelse af

([1]) Revisionen af e-databeskyttelsesdirektivet er en del af en bredere revisionsproces, der tog sigte på oprettelse af en EU-telekommunikationsmyndighed, revision af direktiv 2002/21/EF, 2002/19/EF, 2002/20/EF, 2002/22/EF og 2002/58/EF samt revision af forordning (EF) nr. 2006/2004 (i det følgende samlet benævnt »revision af telekommunikationspakken«).

([2]) Udtalelse af 10. april 2008 om forslaget til et direktiv om ændring af bl.a. direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EUT C 181 af 18.7.2008, s. 1).

([3]) Direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, (forsyningspligtdirektivet) (EFT L 108 af 24.4.2002, s. 51).

([4]) EDPS' bemærkninger til udvalgte spørgsmål, der er rejst i IMCO-betænkningen om revision af direktiv 2002/22/EF (forsyningspligt) og direktiv 2002/58/EF (e-databeskyttelse) af 2. september 2008. Se www.edps.europa.eu

([5]) Europa-Parlamentets lovgivningsmæssige beslutning af 24. september 2008 om forslaget til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om forbrugerbeskyttelsessamarbejde (COM(2007) 698 — C6-0420/2007 — 2007/0248(COD).

bestemmelserne om spam, som det oprindelig blev foreslået i Kommissionens forslag). Efter Parlamentets førstebehandling fulgte Kommissionens vedtagelse af et ændret forslag om e-databeskyttelsesdirektivet (i det følgende benævnt »det ændrede forslag«) ([6]).

5. Rådet nåede den 27. november 2008 til politisk enighed om en revision af bestemmelserne i telekommunikationspakken, herunder e-databeskyttelsesdirektivet, der munder ud i Rådets fælles holdning (»den fælles holdning«) ([7]). Den fælles holdning vil blive forelagt for EP i overensstemmelse med artikel 251, stk. 2, i traktaten om oprettelse af Det Europæiske Fællesskab, hvilket kan indebære ændringsforslag fra EP.

Generelle kommentarer til den fælles holdning

6. Rådet har ændret en række væsentlige elementer i teksten til forslaget og har ikke accepteret mange af de ændringer, som EP havde vedtaget. Til trods for, at den fælles holdning ganske vist som helhed indeholder positive elementer, er EDPS bekymret over indholdet, navnlig fordi den fælles holdning ikke omfatter en række af de positive ændringer, som er foreslået af EP, i det ændrede forslag eller i udtalelserne fra EDPS og de europæiske databeskyttelsesmyndigheder gennem Artikel 29-Gruppen ([8]).

7. Derimod er der i flere tilfælde tale om, at bestemmelser i det ændrede forslag og EP's ændringer, der beskytter borgerne, er udeladt eller svækket i substansen. Som følge heraf er det beskyttelsesniveau, der tilbydes enkeltpersoner i den fælles holdning, væsentligt forringet. Det er grunden til, at EDPS nu afgiver anden udtalelse i håb om, at der i forbindelse med e-databeskyttelsesdirektivets vej igennem lovgivningssystemet vil blive vedtaget nye ændringer, der genetablerer databeskyttelsesbestemmelserne.

8. I anden udtalelse fokuseres der på nogle væsentlige spørgsmål, og alle de punkter, der blev taget op i EDPS' første udtalelse eller i bemærkningerne, vil ikke blive gentaget, idet disse fortsat er gældende. Navnlig følgende emner vil blive taget op i denne udtalelse:

— bestemmelserne om underretning om sikkerhedsbrud

— udvidelse af e-databeskyttelsesdirektivets anvendelsesområde til at omfatte private og offentligt tilgængelige private net

— behandling af trafikdata af hensyn til sikkerheden

— juridiske personers mulighed for at indbringe overtrædelser af e-databeskyttelsesdirektivet for domstolene.

9. I gennemgangen af ovennævnte spørgsmål foretages der i denne udtalelse en analyse af Rådets fælles holdning, idet den sammenholdes med EP's førstebehandlingstekst og Kommissionens ændrede forslag. Udtalelsen omfatter en række anbefalinger, der tager sigte på at strømline bestemmelserne i e-databeskyttelsesdirektivet og sikre, at det fortsat i tilstrækkelig grad beskytter privatlivets fred og personoplysninger.

II. **BESTEMMELSERNE OM UNDERRETNING OM SIKKERHEDSBRUD**

10. EDPS støtter vedtagelsen af et system for underretning om sikkerhedsbrud, hvorefter myndigheder og enkeltpersoner underrettes om, at deres personoplysninger er blevet lækket ([9]). Underretninger om sikkerhedsbrud vil kunne hjælpe privatpersoner til at træffe de nødvendige forholdsregler for at afbøde de skader, som lækagen eventuelt kan medføre. Desuden vil forpligtelsen til at sende underretninger om sikkerhedsbrud tilskynde virksomhederne til at forbedre datasikkerheden, og den vil øge deres ansvarlighed i forbindelse med de personoplysninger, som de har ansvaret for.

11. Kommissionens ændrede forslag, Europa-Parlamentets førstebehandlingstekst og Rådets fælles holdning repræsenterer tre forskellige tilgange til den underretning om sikkerhedsbrud, der er under overvejelse. De indeholder hver især positive aspekter. EDPS er imidlertid af den opfattelse, at de alle kan forbedres, og råder til, at nedennævnte anbefalinger tages i betragtning, når de sidste skridt i retning af en vedtagelse af et system vedrørende sikkerhed overvejes.

([6]) Ændret forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om forbrugerbeskyttelsessamarbejde, KOM(2008) 723 endelig, Bruxelles, den 6. november 2008.

([7]) Findes på Rådets websted.

([8]) Udtalelse 2/2008 om revisionen af direktiv 2002/58/EF om beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet) findes på Artikel 29-Gruppens websted.

([9]) I udtalelsen anvendes udtrykket »lækage« som betegnelse for enhver form for sikkerhedsbrud i forbindelse med personoplysninger som følge af hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles.

12. En gennemgang af de tre systemer for underretning om sikkerhedsbrud viser, at der er fem kritiske punkter, nemlig: *i*) definitionen af »sikkerhedsbrud«, *ii*) de enheder, der er omfattet af underretningspligten (»omfattede enheder«), *iii*) det kriterium, der udløser underretningspligten, *iv*) udpegelse af den enhed, der har ansvaret for at fastslå, om et sikkerhedsbrud opfylder kriteriet, og *v*) modtagerne af underretningen.

Gennemgang af Kommissionens, Rådets og EP's tilgang

13. EP, Kommissionen og Rådet har vedtaget hver sin tilgang til underretning om sikkerhedsbrud. I EP's førstebehandlingstekst ændres det system til underretning om sikkerhedsbrud, der oprindelig var lagt op til i Kommissionens forslag ([10]). I EP's optik finder underretningspligten ikke kun anvendelse på udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, men også på udbydere af informationssamfundstjenester. Desuden vil den nationale tilsynsmyndighed eller de kompetente myndigheder (samlet benævnt »myndighederne«) skulle underrettes om alle brud på persondatasikkerheden efter denne tilgang. Fastslår myndighederne, at der er tale om et *alvorligt* sikkerhedsbrud, vil de kræve, at udbydere af offentligt tilgængelige tjenester og udbydere af informationssamfundstjenester omgående underretter den pågældende. Er der tale om sikkerhedsbrud, der udgør en overhængende og direkte fare, vil alle udbydere skulle underrette enkeltpersonerne, inden de underretter myndigheder, og ikke afvente tilsynsmyndighedernes afgørelse. En undtagelse fra pligten til at underrette forbrugerne gælder enheder, der kan påvise over for myndighederne, at der er anvendt »*passende teknologiske beskyttelsesforanstaltninger*«, der har gjort oplysningerne uforståelige for personer, der ikke må få adgang til dem.

14. Ifølge Rådets tilgang skal såvel abonnenterne som myndighederne underrettes, men kun i de tilfælde, hvor bruddet ifølge den *omfattede enhed* udgør en *alvorlig risiko* for abonnentens privatliv (dvs. identitetstyveri eller identitetsmisbrug, fysisk skade, betydelig tort eller skade af omdømme).

15. I Kommissionens ændrede forslag holdes der fast ved EP's forslag om, at myndighederne skal underrettes om alle tilfælde af sikkerhedsbrud. Det ændrede forslag indeholder imidlertid til forskel fra EP's tilgang en undtagelse fra underretningskravet for så vidt angår enkeltpersoner, hvis udbyderen af en offentligt tilgængelig tjeneste kan påvise over for den kompetente myndighed, at sikkerhedsbruddet »*med rimelig sandsynlighed*« ikke vil føre til *i*) skade (f.eks. økonomisk tab, samfundsmæssig skade eller identitetstyveri), eller at der er anvendt *ii*) »*passende teknologiske beskyttelsesforanstaltninger*« for så vidt angår de oplysninger, som sikkerhedsbruddet vedrører. Kommissionens tilgang indeholder således en skadesbaseret vurdering i forbindelse med de enkelte underretninger.

([10]) Navnlig EP's ændring 187, 124-127 samt 27, 21 og 32 omhandler dette spørgsmål.

16. Det er vigtigt at bemærke, at det ifølge EP's ([11]) og Kommissionens tilgang er *myndighederne*, der i sidste ende skal afgøre, om sikkerhedsbruddet er alvorligt eller med rimelig sandsynlighed vil medføre skade. I modsætning hertil overlades denne afgørelse ifølge Rådets tilgang til de *berørte enheder*.

17. Såvel Rådets som Kommissionens tilgang omfatter kun udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og ikke som EP's tilgang udbydere af informationssamfundstjenester.

Definitionen af »sikkerhedsbrud«

18. EDPS glæder sig over, at de tre lovgivningsforslag indeholder samme definition af underretning i forbindelse med sikkerhedsbrud, der beskrives som »*et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles […]*« ([12]).

19. Som det fremgår af nedenstående hilses denne definition velkommen, fordi den er bred nok til at omfatte de fleste af de situationer, hvor der vil være behov for underretning om sikkerhedsbrud.

20. For det første omfatter definitionen tilfælde, hvor tredjemand har fået *ubeføjet adgang* til personoplysninger, f.eks. ved at hacke en server, der indeholder personoplysninger, og hente sådanne oplysninger.

21. For det andet omfatter denne definition også situationer, hvor personoplysninger er gået tabt eller videregivet, men hvor det endnu ikke er påvist, at der er tale om ubeføjet adgang. Dette omfatter situationer, hvor personoplysningerne er gået tabt (f.eks. cd-rommer, USB-drev eller andre bærbare enheder) eller gjort offentligt tilgængelige af de sædvanlige brugere (en medarbejders datafil, der uforvarende og midlertidigt bliver gjort offentlig tilgængelig på internettet). Da det ofte ikke kan påvises, at tredjemand på et givet tidspunkt har haft ubeføjet adgang til eller ubeføjet har anvendt sådanne oplysninger, vil det være hensigtsmæssigt at lade disse situationer være omfattet af definitionen. EDPS anbefaler derfor, at denne definition bibeholdes. EDPS anbefaler ligeledes, at definitionen af sikkerhedsbrud medtages i artikel 2 i e-databeskyttelsesdirektivet, da det vil være mere i overensstemmelse med den generelle struktur i direktivet og skabe større klarhed.

([11]) Undtagen i tilfælde af overhængende og direkte fare, hvor de omfattede enheder først skal underrette forbrugerne.

([12]) Artikel 2, litra i), i den fælles holdning og det ændrede forslag og artikel 3, stk. 3, i EP's førstebehandlingstekst.

Enheder, der bør være omfattet af underretningspligten

22. Underretningspligten gælder i EP's tilgang for både udbydere af offentligt tilgængelige kommunikationstjenester og udbydere af informationssamfundstjenester. I Rådets og Kommissionens tilgang er det imidlertid kun udbydere af offentligt tilgængelige tjenester som f.eks. telekommunikationsselskaber og internetudbydere, der vil være forpligtet til at underrette enkeltpersoner om sikkerhedsbrud, som fører til lækage af personoplysninger. Andre sektorer, f.eks. online-banker, online-forhandlere, udbydere af online-sundhedstjenester og andre, er ikke omfattet af denne pligt. Af nedennævnte grunde er EDPS af den opfattelse, at det af hensyn til den offentlige orden er afgørende at sikre, at informationssamfundstjenester, der omfatter online-virksomheder, online-banker, udbydere af online-sundhedstjenester m.fl., også er omfattet af kravet om underretning.

23. For det første bemærker EDPS, at telekommunikationsselskaber i høj grad er ofre for sikkerhedsbrud, hvilket berettiger en underretningspligt, men dette gælder også for andre typer virksomheder/udbydere. Online-forhandlere, online-banker og online-apoteker er i lige så stor fare for sikkerhedsbrud som telekommunikationsselskaber, om ikke større. Risikohensynet taler således for, at underretningspligten ikke indskrænkes til kun at gælde udbydere af offentligt tilgængelige elektroniske kommunikationstjenester. Behovet for en bredere tilgang illustreres af de erfaringer, der er gjort i andre lande. F.eks. har stort set samtlige stater i USA (i skrivende stund over 40) vedtaget love om underretning om sikkerhedsbrud, der har et bredere anvendelsesområde og ikke kun omfatter udbydere af offentligt tilgængelige kommunikationstjenester men enhver enhed, der ligger inde med de pågældende personoplysninger.

24. For det andet er der ingen tvivl om, at lækage af den type personoplysninger, som udbydere af offentligt tilgængelige kommunikationstjenester ofte behandler, i høj grad kan få indvirkning på en persons privatliv, hvilket i samme eller endnu højere grad også gør sig gældende for den type personoplysninger, som behandles af udbydere af informationssamfundstjenester. Der er heller ingen tvivl om, at banker og andre finansielle institutioner kan være i besiddelse af meget fortrolige oplysninger (f.eks. om bankkonti), og lækage af sådanne oplysninger kan anvendes til identitetstyveri. Lækage af meget følsomme helbredsrelaterede oplysninger hos online-sundhedstjenester kan ligeledes være særdeles skadende for enkeltpersoner. Der er derfor behov for, at de typer personoplysninger, der kan lækkes, er omfattet af en bredere anvendelse af underretning om sikkerhedsbrud, der som et minimum omfatter udbydere af informationssamfundstjenester.

25. Der er rent juridisk blevet sat spørgsmålstegn ved en udvidelse af denne artikels anvendelsesområde for så vidt angår de enheder, der er underlagt dette krav. Således er den kendsgerning, at e-databeskyttelsesdirektivets generelle anvendelsesområde kun omfatter udbydere af offentligt tilgængelige kommunikationstjenester, blevet anført som en hindring for også at lade underretningspligten gælde udbydere af informationssamfundstjenester.

26. I den forbindelse vil EDPS gerne minde om, *i)* at der rent juridisk ikke er noget til hinder for at lade andre aktører foruden udbydere af offentligt tilgængelige kommunikationstjenester være omfattet af visse af direktivets bestemmelser. Fællesskabslovgiveren har fuld skønsbeføjelse for så vidt angår dette spørgsmål; *ii)* at der i det nugældende e-databeskyttelsesdirektiv er eksempler på anvendelse på andre enheder end udbydere af offentligt tilgængelige tjenester.

27. Eksempelvis finder artikel 13 ikke kun anvendelse på udbydere af offentligt tilgængelige kommunikationstjenester men på enhver virksomhed, der sender uanmodet kommunikation, noget der kræver forudgående samtykke. Endvidere er artikel 5, stk. 3, i e-databeskyttelsesdirektivet, der bl.a. forbyder lagring af data som f.eks. cookies i brugerens terminaludstyr, bindende ikke kun for udbydere af offentligt tilgængelige kommunikationstjenester, men for enhver, der forsøger at lagre information eller opnå adgang til information, der er lagret i privatpersoners terminaludstyr. Desuden har Kommissionen i forbindelse med det nuværende lovgivningsforløb endda foreslået, at anvendelsen af artikel 5, stk. 3, udvides til tilfælde, hvor lignende teknologier (cookies/spionsoftware) ikke kun fremføres via elektroniske kommunikationssystemer, men efter enhver anden metode (distribution ved downloads fra internettet eller via eksterne lagermedier som cd-rommer, USB-nøgler, flashdrev osv.). Alle disse elementer er positive og bør bibeholdes, men er også relevante fortilfælde i den aktuelle diskussion om anvendelsesområdet.

28. I øvrigt har både Kommissionen, EP og Rådet i forbindelse med det nuværende lovgivningsforløb foreslået en ny artikel 6, stk. 6a, jf. nedenfor, der skal finde anvendelse på andre udbydere end udbydere af offentligt tilgængelige kommunikationstjenester.

29. Endelig har borgerne i betragtning af de omfattende positive elementer, som pligten til at underrette om sikkerhedsbrud indebærer, formodentlig også en forventning om, at dette ikke kun gælder, hvis deres personoplysninger bliver lækket af udbydere af offentligt tilgængelige kommunikationstjenester, men også, hvis det sker hos udbydere af informationssamfundstjenester. Borgernes forventninger indfries således ikke, hvis de f.eks. ikke bliver underrettet om, at en online-bank har tabt oplysningerne om deres bankkonti.

30. Summa summarum er EDPS overbevist om, at man kun opnår det fulde udbytte af underretning om sikkerhedsbrud, hvis både udbydere af offentligt tilgængelige kommunikationstjenester og udbydere af informationssamfundstjenester er omfattet.

Kriterium for underretning

31. Med hensyn til hvad der udløser underretning, jf. nedenfor, er EDPS af den opfattelse, at det ændrede forslags kriterium »*med rimelig sandsynlighed vil skade*« er det mest hensigtsmæssige af de tre foreslåede kriterier. Dog er det vigtigt at sikre, at »skade« er tilstrækkelig bredt til at dække alle relevante tilfælde af negative følger for enkeltpersoners privatliv eller andre legitime interesser. Ellers vil det være at foretrække, at der fastsættes et nyt kriterium for obligatorisk underretning, nemlig »*hvis sikkerhedsbruddet med rimelig sandsynlighed vil have negative følger for enkeltpersoner*«.

32. Som nævnt i foregående afsnit er der forskel på, under hvilke omstændigheder enkeltpersoner skal underrettes (omtalt som »udløsende faktor« eller »kriterium«) i EP's, Kommissionens og Rådets tilgang. Mængden af underretninger, enkeltpersoner vil modtage, afhænger naturligvis i vid udstrækning af, hvilken udløsende faktor eller hvilket kriterium for underretning der fastlægges.

33. Ifølge Rådets og Kommissionens tilgang vil der skulle underrettes, hvis sikkerhedsbruddet udgør en »*alvorlig risiko for abonnentens privatliv*« (Rådet), og hvis »*bruddet med rimelig sandsynlighed vil skade forbrugerens interesser*« (Kommissionen). Ifølge EP's tilgang er den udløsende faktor for underretning af enkeltpersoner et spørgsmål om, »*hvor alvorligt sikkerhedsbruddet er*« (dvs. at enkeltpersoner skal underrettes, hvis sikkerhedsbruddet betragtes som »*alvorligt*«). Under denne tærskel kræves der ikke underretning ([13]).

34. EDPS er af den opfattelse, at der, hvis personoplysninger er blevet lækket, kan argumenteres for, at de enkeltpersoner, som oplysningerne omhandler, under alle omstændigheder har ret til at få det at vide. Det er imidlertid kun rimeligt at overveje, om dette er en hensigtsmæssig løsning i lyset af andre interesser og hensyn.

35. Det er blevet nævnt, at pligt til at underrette om alle lækager af personoplysninger, dvs. uden begrænsninger, kunne føre til overdreven underretning og »underretningstræthed«, så brugerne når et mætningspunkt. Som nævnt nedenfor er EDPS opmærksom på denne problemstilling; han ønsker dog samtidig at understrege sin bekymring for, at overdreven underretning godt kan være et tegn på, at praksis på informationssikkerhedsområdet generelt er mangelfuld.

36. Som anført ovenfor erkender EDPS de potentielle negative følger af overdreven underretning og vil gerne medvirke til at sikre, at de retlige rammer, der er vedtaget for underretning om sikkerhedsbrud, ikke fører til et sådant resultat. Såfremt enkeltpersoner ofte ville modtage underretninger om sikkerhedsbrud selv i situationer, hvor der ikke er nogen negative følger, skade eller tort, kan det ende med at underminere et af de centrale mål for underretning, idet enkeltpersoner ironisk nok vil ignorere underretninger i de tilfælde, hvor de faktisk burde træffe foranstaltninger for at beskytte sig selv. Det er derfor vigtigt at finde den rette balance i underretningen, da ordningerne bliver meget mindre effektive, hvis personer ikke reagerer på de underretninger, de modtager.

37. For at kunne vedtage et passende kriterium, der ikke vil føre til overdreven underretning, skal man foruden den udløsende faktor overveje andre faktorer, navnlig definitionen af sikkerhedsbrud og de oplysninger, der er omfattet af underretningspligten. I den forbindelse noterer EDPS sig, at i henhold til de tre foreslåede tilgange kan mængden af underretninger blive stor på baggrund af den brede definition af sikkerhedsbrud, jf. ovenfor. Denne betænkelighed for så vidt angår overdreven underretning forstærkes yderligere af, at definitionen af sikkerhedsbrud omfatter alle former for personoplysninger. Selv om EDPS finder, at dette er det rigtige (at lade underretning omfatte alle typer personoplysninger) i modsætning til andre tilgange, som f.eks. amerikanske love, hvor kravene fokuserer på oplysningernes følsomhed, er det ikke desto mindre en faktor, der skal tages i betragtning.

38. På baggrund af ovenstående og under hensyntagen til de forskellige variabler betragtet under ét finder EDPS, at det er hensigtsmæssigt at indføre en tærskel eller et kriterium, hvorunder det ikke er obligatorisk at give underretning.

39. De foreslåede kriterier, dvs. »*en alvorlig risiko for privatlivets fred*« eller »*med rimelig sandsynlighed vil skade*«, synes begge at omfatte f.eks. samfundsmæssig skade eller skade af omdømme og økonomisk tab. Disse kriterier vil f.eks. tage højde for de tilfælde, hvor en person udsættes for identitetstyveri via udlevering af ikke-offentlige identifikatorer som f.eks. pasnumre, samt afsløring af oplysninger om en persons privatliv. EDPS hilser denne tilgang velkommen. Han er overbevist om, at fordelene ved underretninger om sikkerhedsbrud ikke fuldstændig ville kunne opnås, hvis ordningen kun omfatter brud, der medfører økonomisk tab.

([13]) Jf. fodnote 11 for så vidt angår undtagelsen fra denne regel.

40. Af de to foreslåede kriterier foretrækker EDPS Kommissionens »*med rimelig sandsynlighed vil skade*«, da det vil yde enkeltpersoner et mere hensigtsmæssigt beskyttelsesniveau. Der er meget større sandsynlighed for, at brud kan gøres til genstand for underretning, hvis de »*med rimelig sandsynlighed vil skade*« privatlivets fred, end hvis de udgør »*en alvorlig risiko*« herfor. Det vil derfor i væsentlig grad begrænse antallet af sikkerhedsbrud, der skal anmeldes, hvis kun brud, der udgør en alvorlig risiko for privatlivets fred, er omfattet. Dette ville give udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og udbydere af informationssamfundstjenester en uforholdsmæssigt stor skønsmargen med hensyn til, om det er nødvendigt med en underretning, idet det ville være meget lettere for dem at begrunde en konklusion om, at der ikke er nogen »*alvorlig risiko*«, end om, at det ikke »*med rimelig sandsynlighed vil skade*«. Overdreven underretning skal afgjort undgås, men i det store og hele skal tvivlen komme beskyttelsen af privatlivets fred til gode, og enkeltpersoner bør som et minimum beskyttes, når et brud med rimelig sandsynlighed vil skade dem. Endvidere vil udtrykket »*med rimelig sandsynlighed*« være mere effektivt i praksis, både for omfattede enheder og kompetente myndigheder, da det kræver en objektiv vurdering af sagen og dens relevante sammenhæng.

41. Endvidere kan brud på persondatasikkerheden forårsage skade, der er vanskelig at sætte tal på, og som kan variere. Videregivelse af den samme type oplysninger kan afhængigt af de individuelle omstændigheder skade én person i betydelig grad og en anden person i mindre grad. Et kriterium, der kræver, at skaden skal være materiel, betydelig eller alvorlig, ville ikke være hensigtsmæssig. F.eks. ville Rådets tilgang, der kræver, at sikkerhedsbruddet har en *alvorlig* indvirkning på privatlivets fred, yde utilstrækkelig beskyttelse for den enkelte, idet et sådant kriterium kræver, at indvirkningen på privatlivets fred skal være »alvorlig«. Dette giver også mulighed for en subjektiv vurdering.

42. Udtrykket »*med rimelig sandsynlighed vil skade*« som beskrevet ovenfor synes at være et egnet kriterium for underretning om sikkerhedsbrud, men EDPS mener ikke desto mindre stadig, at det måske ikke omfatter alle de situationer, hvor underretning af enkeltpersoner er berettiget, dvs. alle situationer, hvor der med rimelig sandsynlighed kan forekomme negative følger for enkeltpersoners privatliv eller andre legitime rettigheder. Man kan derfor overveje underretning, »*hvis bruddet med rimelig sandsynlighed vil have negative følger for enkeltpersoner*«.

43. Dette alternative kriterium har den yderligere fordel, at den er i overensstemmelse med EU's databeskyttelseslovgivning. Databeskyttelsesdirektivet omhandler ofte negative følger for de registreredes rettigheder og frihedsrettigheder. For eksempel giver artikel 18 og betragtning 49, som omhandler pligten til at registrere databehandlinger i databeskyttelsesmyndighederne, medlemsstaterne mulighed for at indrømme fritagelse for denne pligt i forbindelse med behandlinger, hvis det »*ikke er sandsynligt, at de registreredes rettigheder og frihedsrettigheder krænkes*«. En lignende affattelse anvendes i artikel 16, stk. 6, i den fælles holdning med henblik på at give juridiske personer mulighed for at anlægge sag mod spammere.

44. Endvidere ville man også på baggrund af ovenstående forvente, at omfattede enheder og navnlig myndigheder, der har kompetence til at håndhæve databeskyttelseslovgivning, har større kendskab til ovennævnte kriterium, og derfor lette dens vurdering af, om et bestemt sikkerhedsbrud opfylder kriteriet.

Enhed, der skal fastslå, om et sikkerhedsbrud opfylder kriteriet

45. I henhold til EP's tilgang (undtagen i tilfælde, hvor der er overhængende fare) og Kommissionens ændrede forslag er det op til medlemsstaternes myndigheder at fastslå, om et sikkerhedsbrud opfylder kriteriet for pligten til at underrette de berørte personer.

46. EDPS finder, at det er vigtigt at inddrage en myndighed, når det skal fastslås, om kriteriet er opfyldt, da dette i en vis udstrækning er en garanti for lovgivningens korrekte anvendelse. Et sådant system kan forebygge, at virksomheder fejlagtigt vurderer sikkerhedsbruddet som ikke værende skadeligt/alvorligt, og derfor undgår at foretage underretning, når en sådan underretning faktisk er nødvendig.

47. På den anden side mener EDPS, at en ordning, hvorefter myndighederne skal foretage vurderingen, måske kan være upraktisk og vanskelig at gennemføre eller i praksis vise sig at virke mod hensigten. Den kan således endda svække databeskyttelsesgarantierne for enkeltpersoner.

48. Med en sådan tilgang er det sandsynligt, at databeskyttelsesmyndighederne vil blive oversvømmet med underretninger om sikkerhedsbrud og vil kunne få alvorlige vanskeligheder med at foretage de nødvendige vurderinger. Det er vigtigt at huske, at for at vurdere, om et sikkerhedsbrud opfylder kriteriet, skal myndighederne have tilstrækkelige interne oplysninger, der ofte er af kompleks teknisk karakter, og som de vil skulle behandle meget hurtigt. Under hensyntagen til vanskelighederne i forbindelse med vurderingen og den kendsgerning, at nogle myndigheder har begrænsede ressourcer, frygter EDPS, at det vil være meget vanskeligt for myndighederne at opfylde denne forpligtelse, og at det vil kunne tage ressourcer fra andre vigtige prioriterede områder. Endvidere vil et sådant system kunne lægge et unødigt pres på myndighederne; hvis de vurderer, at sikkerhedsbruddet ikke er alvorligt og der ikke desto mindre er personer, der lider skade, kunne myndighederne muligvis blive gjort ansvarlige.

49. Denne vanskelighed bliver større, fordi tiden er en vigtig faktor med henblik på at minimere de risici, der er forbundet med sikkerhedsbrud. Medmindre myndighederne kan foretage vurderingen inden for meget korte tidsfrister, kan den ekstra tid, som myndighederne har brug for til at foretage disse vurderinger, øge de skader, som de berørte personer påføres. Dette supplerende trin, der skulle yde større beskyttelse for de enkelte, kan derfor ironisk nok føre til mindre beskyttelse end de systemer, der er baseret på direkte underretning.

50. Af ovennævnte grunde finder EDPS, at det ville være bedre at indføre et system, hvorefter det overlades til de relevante enheder at vurdere, hvorvidt sikkerhedsbruddet opfylder kriteriet, jf. Rådets tilgang.

51. For at undgå en risiko for misbrug, f.eks. i enheder, der undlader at underrette i de tilfælde, hvor underretning klart er påkrævet, er det yderst vigtigt, at der fastsættes visse databeskyttelsesregler, jf. nedenfor.

52. For det første skal den pligt, der gælder for omfattede enheder, til at fastslå, om de skal underrette, naturligvis ledsages af en anden pligt, nemlig obligatorisk underretning af myndighederne om alle sikkerhedsbrud, der opfylder kriteriet. De berørte enheder bør i de tilfælde skulle informere myndighederne om sikkerhedsbruddet og grundene til deres beslutning om underretningen samt indholdet af eventuelle underretninger.

53. For det andet skal myndighederne have en reel tilsynsrolle. I forbindelse med udførelsen af denne rolle skal myndighederne have mulighed for, men ikke pligt til, at undersøge omstændighederne omkring sikkerhedsbruddet og kræve de afhjælpende foranstaltninger, der måtte være hensigtsmæssige ([14]). Dette bør ikke kun omfatte underretning af enkeltpersoner (hvis dette endnu ikke har fundet sted), men også muligheden for at pålægge en pligt til at træffe foranstaltninger til at forebygge yderligere sikkerhedsbrud. Myndighederne bør have effektive beføjelser og ressourcer hertil og det nødvendige spillerum til at beslutte, hvornår der skal reageres på en underretning om sikkerhedsbrud. Med andre ord ville det give myndighederne mulighed for at være selektive og indlede efterforskninger af f.eks. omfattende og meget skadelige sikkerhedsbrud, idet overholdelse af lovgivningens krav kontrolleres og håndhæves.

([14]) I artikel 15a, stk. 3, anerkendes disse tilsynsbeføjelser, idet følgende fastsættes: »Medlemsstaterne sikrer, at kompetente nationale myndigheder, og, hvor det er relevant, andre nationale organer, har alle nødvendige beføjelser og ressourcer til efterforskning, herunder mulighed for at skaffe sig relevante oplysninger, som de måtte have brug for under overvågningen og håndhævelsen af nationale bestemmelser, der er vedtaget i medfør af dette direktiv.«.

54. For at opnå ovenstående, f.eks. i artikel 15a, stk. 3, og databeskyttelsesdirektivet, anbefaler EDPS, at der ud over de beføjelser, der er anerkendt i e-databeskyttelsesdirektivet, indføjes følgende tekst: »*Hvis abonnenten eller den berørte person ikke allerede er blevet underrettet, kan den kompetente nationale myndighed efter at have overvejet sikkerhedsbruddets karakter pålægge udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester eller udbyderne af informationssamfundstjenester at foretage underretningen*«.

55. Endvidere henstiller EDPS til EP og Rådet, at de bekræfter den af EP foreslåede pligt (ændring 122, artikel 4, stk. 1a) for enheder til at gennemføre risikovurdering og identifikation i deres systemer og de personoplysninger, som de har til hensigt at behandle. På grundlag af denne pligt skal enhederne udarbejde en skræddersyet og præcis definition af de sikkerhedsforanstaltninger, som vil finde anvendelse i deres tilfælde, og som skal være tilgængelig for myndighederne. Hvis der sker et sikkerhedsbrud, vil denne pligt hjælpe de omfattede enheder - og senere også myndighederne i deres tilsynsrolle - med at afgøre, om lækagen af sådanne oplysninger kan have negative følger for eller skade enkeltpersoner.

56. For det tredje skal omfattede enheders pligt til at afgøre, om de skal underrette enkeltpersoner, ledsages af en pligt til at opretholde et detaljeret og omfattende internt kontrolspor, som beskriver alle de sikkerhedsbrud, der er sket, og alle underretninger derom samt alle foranstaltninger, der er truffet for at undgå fremtidige sikkerhedsbrud. Dette interne kontrolspor skal være tilgængeligt for myndighederne med henblik på gennemgang og eventuelt efterforskning. Dette vil give myndighederne mulighed for at udføre deres tilsynsrolle. Dette kan opnås ved at vedtage en tekst med f.eks. følgende ordlyd: »*Udbyderne af offentligt tilgængelige kommunikationstjenester og udbyderne af informationssamfundstjenester skal føre og opretholde omfattende fortegnelser over alle sikkerhedsbrud, relevante tekniske oplysninger i den forbindelse og trufne afhjælpende foranstaltninger. Fortegnelserne skal også indeholde en henvisning til alle underretninger til abonnenter eller berørte enkeltpersoner og til de kompetente nationale myndigheder, herunder dato og indhold. Fortegnelserne skal efter anmodning forelægges den kompetente nationale myndighed.*«

57. For at sikre en ensartet gennemførelse af dette kriterium samt andre relevante aspekter af rammerne for sikkerhedsbrud, såsom former og procedurer for underretningen, ville det naturligvis være hensigtsmæssigt, at Kommissionen efter høring af EDPS, Artikel 29-Gruppen og relevante interesseparter vedtager tekniske gennemførelsesforanstaltninger.

Modtagere af underretningen

58. Hvad angår modtagere af underretningerne foretrækker EDPS EP's og Kommissionens terminologi frem for Rådets. EP har erstattet ordet »abonnenter« med ordet »brugere«. Kommissionen anvender »abonnenter« og »berørt person«. Både EP's og Kommissionens affattelse ville omfatte både nuværende abonnenter og tidligere abonnenter og tredjeparter, som f.eks. brugere, der arbejder sammen med nogle omfattede enheder uden at være abonnenter. EDPS hilser denne tilgang velkommen og opfordrer EP og Rådet til at bevare den.

59. EDPS noterer sig imidlertid en række uoverensstemmelser i terminologien i EP's førstebehandling, der bør ordnes. For eksempel er ordet »abonnent« i de fleste tilfælde, men ikke i alle, blevet erstattet med ordet »bruger« og i andre tilfælde med ordet »forbruger«. Dette bør harmoniseres.

III. **E-DATABESKYTTELSESDIREKTIVETS ANVENDELSESOMRÅDE: OFFENTLIGE OG PRIVATE NET**

60. Artikel 3, stk. 1, i det nuværende e-databeskyttelsesdirektiv fastsætter de enheder, der primært er omfattet af direktivet, dvs. dem, der behandler oplysninger »*i forbindelse med*«, at offentlige elektroniske kommunikationstjenester stilles til rådighed via offentlige net ([15]). Eksempler på aktiviteter, der udøves af udbydere af offentlige kommunikationstjenester i offentlige net, omfatter ydelse af adgang til internettet, transmission af oplysninger via elektroniske net, mobiltelefonforbindelser og telefonforbindelser, osv.

61. EP har vedtaget ændring 121, der ændrer artikel 3 i Kommissionens oprindelige forslag, hvorefter e-databeskyttelsesdirektivets anvendelsesområde udvides til at omfatte »*behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige og private kommunikationsnet og offentligt tilgængelige private net i Fællesskabet, […]*« (artikel 3, stk. 1, i e-databeskyttelsesdirektivet). Desværre har Rådet og Kommissionen fundet det vanskeligt at acceptere denne ændring og har derfor ikke indarbejdet den i den fælles holdning og det ændrede forslag.

E-databeskyttelsesdirektivets anvendelse på offentligt tilgængelige private net

62. Af de årsager, der er omhandlet nedenfor, og for at medvirke til at fremme konsensus opfordrer EDPS til, at substansen i ændring 121 bevares. Desuden foreslår EDPS, at der medtages en ændring, der skal medvirke til yderligere at præcisere de typer tjenester, der vil være omfattet af det udvidede anvendelsesområde.

63. Private net anvendes ofte til at levere elektroniske kommunikationstjenester, som f.eks. internetadgang, til et ubestemt antal personer, der potentielt kan være stort. Dette er for eksempel tilfældet med internetadgang på internetcaféer samt WiFi-hotspots, der er tilgængelige i hoteller, restauranter, lufthavne, tog og andre strukturer, der er åbne for offentligheden, og hvor sådanne tjenester ofte udbydes som et supplement til andre tjenester (drikkevarer, logi, osv.).

64. I alle ovennævnte eksempler stilles en kommunikationstjeneste, f.eks. internetadgang, ikke til rådighed for offentligheden via et offentligt net, men via et net, der kan betragtes som privat, dvs. et privat drevet net. Selv om kommunikationstjenesten i ovennævnte tilfælde stilles til rådighed for offentligheden, er udbydelse af disse tjenester faktisk ikke omfattet af hele e-databeskyttelsesdirektivet eller i det mindste af nogle af dets artikler, fordi den anvendte type net snarere er privat end offentlig. ([16]). Som følge heraf er de grundlæggende rettigheder for enkeltpersoner, der sikres ved e-databeskyttelsesdirektivet, ikke beskyttet i disse situationer, og der skabes en anden retssituation for brugere, der har adgang til de samme internetadgangstjenester via offentlige telekommunikationsmidler end for dem, der har adgang via private. Dette til trods for at der i alle disse tilfælde eksisterer en risiko for personens privatliv og personoplysninger i samme omfang, som når offentlige net anvendes til at levere tjenesten. Kort sagt synes der ikke at være en logisk begrundelse for i direktivet at behandle kommunikationstjenester, der udbydes via et privat net, anderledes end dem, der udbydes via et offentligt net.

65. EDPS vil derfor støtte en ændring, som f.eks. EP's ændring 121, hvorefter e-databeskyttelsesdirektivet også vil finde anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via *private* kommunikationsnet.

66. EDPS erkender imidlertid, at denne formulering ville kunne få uforudselige og eventuelt utilsigtede konsekvenser. Blot det, at private net nævnes, ville kunne

([15]) »Dette direktiv finder anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet«.

([16]) Derimod kan det anføres, at da kommunikationstjenesterne leveres til offentligheden, selv om nettet er privat, er leveringen af sådanne tjenester omfattet af de eksisterende retlige rammer på trods af, at nettet er privat. I Frankrig anses arbejdsgivere, der giver deres ansatte internetadgang, f.eks. for at svare til udbydere af internetadgang, der tilbyder internetadgang på kommercielt grundlag. Denne fortolkning er ikke almindeligt accepteret.

fortolkes sådan, at situationer, som det tydeligvis ikke er hensigten, at direktivet skal omfatte, er omfattet. Det kunne f.eks. hævdes, at en bogstavelig eller streng fortolkning af denne formulering kunne medføre, at ejere af boliger udstyret med WiFi ([17]), der gør det muligt for alle inden for deres rækkevidde (normalt boligen) at tilslutte sig, falder ind under direktivets anvendelsesområde, selv om dette ikke er hensigten med ændring 121. For at undgå dette foreslår EDPS, at ændring 121 omformuleres, således at der under e-databeskyttelsesdirektivets anvendelsesområde medtages »*behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige eller offentligt tilgængelige private kommunikationsnet i Fællesskabet,* …«

67. Dette ville bidrage til at tydeliggøre, at kun private net, der er offentligt tilgængelige, vil være omfattet af e-databeskyttelsesdirektivet. Ved *kun* at anvende e-databeskyttelsesdirektivets bestemmelser på *offentligt tilgængelige private net* (og ikke på alle private net) fastsættes der en grænse, således at direktivet kun vil omfatte kommunikationstjenester, der udbydes via private net, og som bevidst gøres *tilgængelige* for offentligheden. Denne formulering vil yderligere medvirke til at understrege, at private nets *tilgængelighed for offentligheden i almindelighed* er en afgørende faktor for, om de er omfattet af direktivet (ud over levering af en offentlig tilgængelig kommunikationstjeneste). Med andre ord ville denne type tjeneste/net være omfattet af e-databeskyttelsesdirektivet, uanset om nettet er offentligt eller privat, hvis nettet bevidst gøres tilgængeligt for offentligheden for at yde en offentlig kommunikationstjeneste, som f.eks. internetadgang, selv om en sådan tjeneste er et supplement til en anden (f.eks. hotelophold).

68. EDPS gør opmærksom på, at den tilgang, der gives tilslutning til ovenfor, og hvorefter bestemmelserne i e-databeskyttelsesdirektivet finder anvendelse på *offentligt tilgængelige private net*, stemmer overens med de tilgange, der anvendes i flere medlemsstater, hvor myndighederne allerede anser sådanne typer tjenester samt tjenester, der ydes via rent private net, for at høre under anvendelsesområdet for de nationale bestemmelser, der gennemfører e-databeskyttelsesdirektivet ([18]).

69. For at fremme retssikkerheden for så vidt angår enheder, der er omfattet af det nye anvendelsesområde, kan det være nyttigt at indføje en ændring i e-databeskyttelsesdirektivet, der definerer »offentligt tilgængelige private net«, og som kunne affattes således: »*offentligt tilgængeligt privat net: et privat drevet net, som offentligheden i almindelighed normalt har uindskrænket adgang til, uanset om det sker mod betaling eller ej eller i tilknytning til andre tjenester eller tilbud, med forbehold af accept af de gældende betingelser.*«

70. I praksis ville ovenstående tilgang indebære, at private net i hoteller og andre strukturer, der giver offentligheden i almindelighed adgang til internettet via et privat net, er omfattet. Omvendt vil udbud af kommunikationstjenester via rent private net, hvor tjenesten omfatter en begrænset gruppe af identificerbare fysiske personer, ikke være omfattet. Derfor vil f.eks. virtuelle private net og forbrugeres hjem, der er udstyret med WiFi, ikke være omfattet af direktivet. Tjenester, der udbydes via net, der udelukkende er virksomhedsnet, vil heller ikke være omfattet.

Private net, der er omfattet af e-databeskyttelsesdirektivets anvendelsesområde

71. Undtagelse af private net generelt som foreslået ovenfor bør anses for at være en midlertidig foranstaltning, der bør gøres til genstand for yderligere drøftelser. Under hensyn til på den ene side konsekvenserne for privatlivets fred, hvis rent private net som sådan undtages, og på den anden side den kendsgerning, at det berører et stort antal mennesker, som normalt har adgang til internettet via virksomhedsnet, skal dette tages op til fornyet overvejelse i fremtiden. Af denne årsag samt for at fremme drøftelserne om dette emne anbefaler EDPS, at der indsættes en betragtning i e-databeskyttelsesdirektivet, i henhold til hvilken Kommissionen vil gennemføre en offentlig høring om anvendelsen af e-databeskyttelsesdirektivet på alle private net, med input fra EDPS, databeskyttelsesmyndighederne og andre relevante interesseparter. Desuden kunne det i betragtningen præciseres, at Kommissionen på baggrund af den offentlige høring bør fremsætte et passende forslag om at lade flere eller færre typer enheder være omfattet af e-databeskyttelsesdirektivet.

72. Desuden bør de forskellige artikler i e-databeskyttelsesdirektivet ændres i overensstemmelse dermed, således at der i alle operationelle bestemmelser udtrykkeligt nævnes offentligt tilgængelige private net foruden offentlige net.

IV. **BEHANDLING AF TRAFIKDATA AF HENSYN TIL SIKKERHEDEN**

73. Under lovgivningsforløbet i forbindelse med revisionen af e-databeskyttelsesdirektivet har virksomheder, der udbyder sikkerhedstjenester, anført at det er nødvendigt, at der i e-databeskyttelsesdirektivet indføjes en bestemmelse, der lovliggør indsamlingen af trafikdata for at garantere effektiv onlinesikkerhed.

([17]) Typisk trådløse lokalnet (LAN).
([18]) Jf. fodnote 16.

74. Som følge heraf har EP indsat ændring 181 om et nyt artikel 6, stk. 6a, der udtrykkeligt giver tilladelse til at behandle trafikdata af hensyn til sikkerheden: »*Uanset overholdelsen af andre bestemmelser end artikel 7 i direktiv 95/46/EF og dette direktivs artikel 5 kan trafikdata behandles i den registeransvarliges legitime interesse med det formål at implementere tekniske foranstaltninger for at garantere net- og informationssikkerheden som defineret i artikel 4, litra c, i Europa-Parlamentets og Rådets forordning af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed, af en offentlig elektronisk kommunikationstjeneste, et offentligt eller privat elektronisk kommunikationsnet, en informationssamfundstjeneste eller terminaludstyr og elektronisk kommunikationsudstyr forbundet hermed, undtagen hvor sådanne interesser overskygges af den registreredes interesser, hvad angår grundlæggende rettigheder og friheder. Behandlingen må kun omfatte det strengt nødvendige i forbindelse med sikkerhedsaktiviteten.*«

75. Kommissionens ændrede forslag accepterede i princippet denne ændring, men udelod en central bestemmelse, der skulle sikre, at direktivets andre bestemmelser overholdes, idet »*Uanset overholdelsen (…) direktivs artikel 5*« blev udeladt. Rådet vedtog en ændret udgave, der yderligere udvandede den vigtige beskyttelse og afvejningen af interesser i ændring 181, og som er affattet således: […] »*Trafikdata kan behandles, […] i det omfang det er strengt nødvendigt for at […] garantere net- og informationssikkerheden som defineret i artikel 4, litra c, i Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed […]*«.

76. Som nævnt nedenfor er artikel 6, stk. 6a, overflødigt og risikerer at blive misbrugt, navnlig hvis det vedtages i en form, der ikke omfatter den vigtige beskyttelse, klausuler om overholdelse af andre bestemmelser i direktivet og afvejningen af forskellige hensyn. EDPS anbefaler derfor, at denne artikel forkastes, eller at det som minimum sikres, at en artikel af denne art og om dette spørgsmål omfatter den beskyttelse, der var indeholdt i ændring 181 som vedtaget af EP.

Juridiske grundlag for behandling af trafikdata, der finder anvendelse på udbydere af elektroniske kommunikationstjenester og andre registeransvarlige i den nugældende databeskyttelseslovgivning

77. Artikel 6 i e-databeskyttelsesdirektivet indeholder bestemmelser om, i hvilket omfang udbydere af offentligt tilgængelige elektroniske kommunikationstjenester lovligt må behandle trafikdata, og trafikdata kan kun behandles med et begrænset antal formål som f.eks. fakturering, samtrafik og markedsføring. Behandlingen må kun finde sted på specifikke betingelser, f.eks. med enkeltpersonernes samtykke, når det drejer sig om markedsføring. Herudover må andre registeransvarlige, som f.eks. udbydere af informationssamfundstjenester, behandle trafikdata i henhold til artikel 7 i databeskyttelsesdirektivet, ifølge hvilken registeransvarlige må behandle personoplysninger, hvis de har hjemmel hertil i mindst én af de på en liste opregnede juridiske grundlag.

78. Et eksempel på hjemmel findes i artikel 7, litra a), i databeskyttelsesdirektivet, hvorefter den registreredes samtykke kræves. F.eks. skal en online-forhandler, der ønsker at behandle trafikdata med henblik på fremsendelse af reklame- eller markedsføringsmateriale, have personens samtykke. En anden form for hjemmel i artikel 7 gives f.eks. til virksomheder, der tilbyder sikkerhedstjenester, så de i visse tilfælde har lov til at behandle trafikdata af hensyn til sikkerheden. Dette bygger på artikel 7, litra f), hvori det hedder, at registeransvarlige må behandle personoplysninger, hvis behandlingen er »*nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder (…) går forud herfor …*« Databeskyttelsesdirektivet indeholder ikke nærmere bestemmelser om, hvornår behandling af personoplysninger opfylder dette krav. Det er i stedet den registeransvarliges afgørelse i de enkelte tilfælde, ofte med de nationale databeskyttelsesmyndigheders og andre myndigheders samtykke.

79. Dette samspil mellem artikel 7 i databeskyttelsesdirektivet og det foreslåede artikel 6, stk. 6a, i e-databeskyttelsesdirektivet bør tages i betragtning. Det foreslåede artikel 6, stk. 6a, er en udspecificering af, under hvilke omstændigheder kravene i artikel 7, litra f), jf. ovenfor, er opfyldt. Ved at tillade behandling af trafikdata som bidrag til at garantere net- og informationssikkerheden giver artikel 6, stk. 6a, den registeransvarlige mulighed for en sådan behandling med det formål at forfølge en legitim interesse.

80. Som forklaret nedenfor er det EDPS' opfattelse, at det foreslåede artikel 6, stk. 6a, hverken er nødvendigt eller nyttigt. Fra et juridisk synspunkt er det i princippet helt unødvendigt at fastslå, om en bestemt type databehandling, i dette tilfælde behandling af trafikdata af hensyn til sikkerheden, opfylder kravene i artikel 7, litra f), i databeskyttelsesdirektivet, fordi personens samtykke kan være nødvendigt, jf. artikel 7, litra a). Som tidligere nævnt foretages denne vurdering normalt af den registeransvarlige, dvs. på gennemførelsesplan, af virksomheder i samråd med databeskyttelsesmyndighederne og i nødvendigt omfang af domstolene. Generelt er det EDPS' opfattelse, at lovlig behandling af trafikdata af hensyn til sikkerheden i visse tilfælde, når den foretages uden at bringe enkeltpersoners grundlæggende rettigheder og frihedsrettigheder i fare, må siges at opfylde kravene i artikel 7, litra f), i databeskyttelsesdirektivet og derfor kan foretages. Endvidere er der ikke hverken i databeskyttelsesdirektivet eller

e-databeskyttelsesdirektivet nogen eksempler på fremhævelse eller særbehandling af visse former for databehandling, der opfylder kravene i artikel 7, litra f), og der har heller ikke været noget påvist behov for en sådan undtagelse. Derimod virker det som tidligere nævnt, som om denne type behandling i mange tilfælde falder fint ind under den nuværende tekst. En lovbestemmelse, der bekræfter denne vurdering, er derfor i princippet overflødig.

EP's, Rådets og Kommissionens udgave af artikel 6, stk. 6a

81. Som nævnt ovenfor er det dog vigtigt at understrege, at ændring 181 som vedtaget af EP - omend overflødig - imidlertid i en vis udstrækning er affattet under hensyn til principperne om beskyttelse af privatlivets fred og databeskyttelse i databeskyttelseslovgivningen. EP's ændring 181 kunne i højere grad afspejle hensynet til databeskyttelse og privatlivets fred, hvis man f.eks. tilføjede »i specifikke tilfælde« for at sikre, at denne artikel kun finder anvendelse i udvalgte tilfælde, eller ved tilføjelse af en specifik lagringsperiode.

82. Ændring 181 indeholder visse positive elementer. Det bekræftes deri, at behandlingen skal opfylde andre principper for databeskyttelse i forbindelse med behandling af personoplysninger (»*Uanset overholdelsen af andre bestemmelser end artikel 7 i direktiv 95/46/EF og dette direktivs artikel […]*«). Endvidere finder ændring 181, selvom den giver mulighed for behandling af trafikdata af hensyn til sikkerheden, en balance mellem interesserne hos den enhed, der behandler trafikdataene, og hos de personer, hvis data behandles, så databehandlingen kun kan ske, hvis personernes grundlæggende frihedsrettigheder ikke overskygges af den databehandlende enheds interesser (»*undtagen hvor sådanne interesser overskygges af den registreredes interesser, hvad angår grundlæggende frihedsrettigheder*«). Dette krav er afgørende, da det kan give mulighed for behandling af trafikdata i specifikke tilfælde; det giver dog ikke en enhed lov til at behandle trafikdata i stor stil.

83. Rådets ændrede udgave af ændringen indeholder positive elementer, f.eks. det, at der holdes fast i udtrykket »*strengt nødvendigt*«, hvorved artiklens begrænsede anvendelsesområde understreges. I Rådets udgave har man imidlertid udeladt ovennævnte data- og privatlivsbeskyttende bestemmelser. Selv om almindelige databeskyttelsesbestemmelser i princippet finder anvendelse, uanset om der specifikt henvises til dem i de enkelte tilfælde, kan Rådets udgave af artikel 6, stk. 6a, ikke desto mindre fortolkes således, at der gives fuld skønsmæssig beføjelse til at behandle trafikdata uden nogen krav om overholdelse af de data- og privatlivsbeskyttende bestemmelser, der gælder i forbindelse med behandling af trafikdata. Man kan derfor hævde, at trafikdata må indsamles, lagres og anvendes, uden at man skal overholde de databeskyttelsesprincipper og specifikke forpligtelser, de ansvarlige parter normalt er underlagt, f.eks. kvalitetsprincippet eller pligten til at sikre en rimelig og lovlig behandling og til at holde oplysningerne hemmelige og sikre. Desuden kan Rådets udgave, fordi der hverken er anført gældende databeskyttelsesprincipper, der fastsætter tidsfrister for lagring af oplysninger, eller specifikke tidsfrister i artiklen, fortolkes således, at trafikdata må indsamles og behandles til sikkerhedsformål uden tidsbegrænsning.

84. Rådet har desuden svækket beskyttelsen af privatlivets fred i visse dele af teksten ved at gøre formuleringen bredere. For eksempel er henvisningen til »*den registeransvarliges legitime interesser*« udgået, hvilket skaber tvivl om, hvilken type enheder der er omfattet af denne undtagelse. Det er yderst vigtigt at undgå at åbne op, så alle brugere eller juridiske enheder kan udnytte ændringen.

85. De seneste erfaringer i EP og Rådet viser, at det er vanskeligt at lovgive om, i hvilket omfang og under hvilke omstændigheder behandling af data af hensyn til sikkerheden kan ske lovligt. Det tyder ikke på, at nogen gældende eller fremtidige artikler kan fjerne den klare risiko, der er for, at denne undtagelse anvendes for bredt af andre end rent sikkerhedsmæssige årsager, eller af enheder, der ikke skulle være omfattet. Det betyder ikke, at en sådan behandling ikke finder sted alligevel. Om og i hvilket omfang det kan ske, kan dog bedre vurderes på gennemførelsesplan. Enheder, der ønsker at foretage en sådan behandling, bør drøfte omfang og betingelser med databeskyttelsesmyndighederne og eventuelt med Artikel 29-Gruppen. Alternativt kunne e-databeskyttelsesdirektivet indeholde en artikel, der giver mulighed for at behandle trafikdata af hensyn til sikkerheden med forbehold af udtrykkelig tilladelse hertil fra databeskyttelsesmyndighederne.

86. Tages der på den ene side hensyn til de risici, som artikel 6, stk. 6a, kan medføre for det enkelte menneskes grundlæggende ret til beskyttelse af oplysninger og privatliv, og på den anden side den kendsgerning, at artiklen som nævnt i denne udtalelse fra et juridisk synspunkt er overflødig, må EDPS konkludere, at den bedste løsning vil være helt at udelade det foreslåede artikel 6, stk. 6a.

87. Vedtages der en tekst, hvis ordlyd svarer til den nuværende udgave af artikel 6, stk. 6a, trods EDPS' anbefaling om det modsatte, bør den som et minimum indeholde ovennævnte databeskyttelsesbestemmelser. Den bør ligeledes anbringes hensigtsmæssigt i den nuværende opbygning af artikel 6, helst som nyt stk. 2a.

V. **JURIDISKE PERSONERS MULIGHED FOR AT INDBRINGE OVERTRÆDELSER AF E-DATABESKYTTELSESDIREKTIVET FOR DOMSTOLENE**

88. EP har vedtaget ændring 133, der giver udbydere af internetadgang og andre juridiske enheder som f.eks. forbrugerorganisationer mulighed for at indbringe overtrædelser af bestemmelserne i e-databeskyttelsesdirektivet for domstolen ([19]). Desværre har hverken Kommissionen eller Rådet accepteret den. EDPS finder denne ændring meget positiv og anbefaler, at den bevares.

89. For at forstå betydningen af denne ændring er man nødt til at indse, at på området beskyttelse af privatlivets fred og databeskyttelse er den skade, en person udsættes for individuelt set, normalt ikke i sig selv tilstrækkelig til, at han/hun indbringer sagen for domstolene. Enkeltpersoner går normalt ikke selv til domstolene, fordi de modtager spam, eller fordi deres navn er blevet uretmæssigt opført på en adresseliste. Denne ændring vil give forbruger- og handelsorganisationer, der repræsenterer forbrugernes interesser på et kollektivt plan, mulighed for at indbringe sager for domstolene på deres vegne. Flere forskellige håndhævelsesmekanismer kan også tænkes at tilskynde til et højere overholdelsesniveau og er derfor til fordel for en effektiv anvendelse af bestemmelserne i e-databeskyttelsesdirektivet.

90. Der er juridisk præcedens i nogle medlemsstaters retlige rammer, der allerede giver kollektiv klageadgang for at give forbrugere eller interessegrupper mulighed for at fremsætte erstatningskrav over for skadevolder.

91. Desuden giver nogle medlemsstaters konkurrencelove ([20]) forbrugere, interessegrupper (foruden den *berørte konkurrent*) ret til at anlægge sag mod den overtrædende enhed. Baggrunden er, at virksomheder, der overtræder konkurrencelovene, sandsynligvis vil drage fordel heraf, eftersom forbrugere, der kun lider ubetydelig skade, generelt tøver med at anlægge sag. Dette gælder tilsvarende på området databeskyttelse og privatlivets fred.

92. Som nævnt ovenfor, fremmer det forbrugernes stilling, og generel overholdelse af databeskyttelseslovgivningen, hvis juridiske enheder som f.eks. forbrugerorganisationer og udbydere af elektroniske kommunikationstjenester i offentlige net får ret til at anlægge sag. Hvis lovovertrædende virksomheder har en større risiko for at blive sagsøgt, vil de sandsynligvis investere mere i at overholde databeskyttelseslovgivningen, hvilket i det lange løb øger niveauet for beskyttelse af privatlivets fred og forbrugerne. Af alle disse grunde opfordrer EDPS EP og Rådet til at vedtage en bestemmelse, der gør det muligt for juridiske enheder mulighed for at indbringe spørgsmål om overtrædelser af bestemmelserne i e-databeskyttelsesdirektivet for domstolene.

([19]) Artikel 13, stk. 6, i EP's førstebehandlingstekst.
([20]) Se f.eks. § 8 UWG — tysk lov om illoyal konkurrence.

VI. **KONKLUSION**

93. Rådets fælles holdning, EP's førstebehandling og Kommissionens ændrede forslag indeholder i varierende grad positive elementer, der kan være med til at styrke beskyttelsen af enkeltpersoners privatliv og personoplysninger.

94. EDPS mener imidlertid, at de kan forbedres, navnlig Rådets fælles holdning, der desværre ikke indeholder nogle af de ændringer fra EP, der skulle medvirke til at sikre tilstrækkelig beskyttelse af enkeltpersoners privatliv og personoplysninger. EDPS opfordrer EP og Rådet til at genindføre de garantier for beskyttelse af privatlivets fred, der var indbygget i EP's førstebehandlingstekst.

95. Desuden mener EDPS, at det vil være hensigtsmæssigt at strømline nogle af direktivets bestemmelser. Det gælder især bestemmelserne om sikkerhedsbrud, eftersom EDPS mener, at man bedst opnår den fulde fordel af underretning om sikkerhedsbrud, hvis den retlige ramme er fastlagt lige fra starten. Endelig mener EDPS, at det vil være hensigtsmæssigt at forbedre og præcisere formuleringen af nogle af direktivets bestemmelser.

96. I lyset af ovenstående tilskynder EDPS EP og Rådet til at øge deres indsats for at forbedre og præcisere nogle af bestemmelserne i e-databeskyttelsesdirektivet og samtidig genindsætte de ændringer, som EP vedtog under førstebehandlingen, for at garantere et tilstrækkeligt niveau for beskyttelse af privatlivets fred og personoplysninger. Med henblik herpå sammenfatter punkt 97, 98, 99 og 100 nedenfor de spørgsmål, der er tale om, og indeholder nogle henstillinger og formuleringsforslag. EDPS opfordrer alle involverede parter til at tage dem i betragtning, efterhånden som e-databeskyttelsesdirektivet går i retning af endelig vedtagelse.

Sikkerhedsbrud

97. EP, Kommissionen og Rådet har hver især vedtaget en tilgang til underretning om sikkerhedsbrud. Der er forskelle mellem de tre modeller, bl.a. med hensyn til de enheder, der er omfattet af forpligtelsen, kriteriet eller den udløsende faktor for underretningen, de registrerede, der har ret til at blive underrettet osv. EP og Rådet skal gøre deres yderste for at udforme en solid retlig ramme for sikkerhedsbrud. Med henblik herpå henstilles følgende til EP og Rådet:

— definitionen af sikkerhedsbrud i EP's, Rådets og Kommissionens tekster bør *fastholdes*, da den er bred nok til at omfatte de fleste af de situationer, hvor der vil være behov for underretning om sikkerhedsbrud.

— Udbydere af informationssamfundstjenester bør være *omfattet* af de foreslåede underretningskrav. Online-forhandlere, online-banker og online-apoteker er i lige så stor fare for sikkerhedsbrud som telekommunikationsselskaber, om ikke større. Borgere vil forvente at blive underrettet, ikke kun når udbydere af internetadgang udsættes for sikkerhedsbrud, men navnlig, når dette sker for deres online-banker og online-apoteker.

— med hensyn til den udløsende faktor for underretning er kriteriet i det ændrede forslag »*med rimelig sandsynlighed vil skade*« et hensigtsmæssigt kriterium, der betyder, at ordningen fungerer. Dog er det vigtigt at sikre, at »skade« er tilstrækkelig bredt til at dække alle relevante tilfælde af negative følger for enkeltpersoners privatliv eller andre legitime interesser. Ellers vil det være at foretrække, at der fastsættes et nyt kriterium, der gør underretning obligatorisk, »*hvis bruddet med rimelig sandsynlighed vil have negative følger for enkeltpersoner*«. Rådets tilgang, der kræver, at bruddet har en *alvorlig* indvirkning på privatlivets fred, vil yde utilstrækkelig beskyttelse for enkeltpersoner, idet et sådant kriterium kræver, at indvirkningen på privatlivets fred skal være »alvorlig«. Dette giver også mulighed for en subjektiv vurdering.

— Selv om det bestemt har positive virkninger, at en myndighed inddrages i at fastslå, om en berørt enhed skal underrette enkeltpersoner, kan det være upraktisk og vanskeligt at gennemføre og kan også tage ressourcer fra andre vigtige prioriterede områder. Hvis myndighederne ikke kan reagere ekstremt hurtigt, er EDPS bange for, at et sådant system oven i købet kan mindske beskyttelsen af enkeltpersoner og lægge unødigt pres på myndighederne. Således anbefaler EDPS generelt, at *der indføres* et system, hvor det er op til de berørte enheder at foretage vurderingen af, om de skal underrette.

— for at gøre det muligt for myndighederne at få overblik over de vurderinger, som de omfattede enheder foretager med hensyn til, om der skal underrettes, bør der *fastsættes* følgende sikkerhedsbestemmelser

  — *det bør sikres*, at sådanne enheder er forpligtet til at underrette myndighederne om alle sikkerhedsbrud, der opfylder kriteriet

  — myndighederne bør *tildeles* en tilsynsrolle, der gør det muligt for dem at være selektive for at være effektive. For at opnå dette indsættes følgende tekst: »*Hvis abonnenten eller den berørte person ikke allerede er blevet underrettet, kan den kompetente nationale myndighed efter at have overvejet sikkerhedsbruddets karakter pålægge udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester eller udbyderne af informationssamfundstjenester at foretage underretningen*«.

  — *der bør vedtages* en ny bestemmelse om, at enheder skal opretholde et detaljeret og omfattende internt revisionsspor. Dette kan opnås ved at vedtage følgende tekst: »*Udbyderne af elektroniske kommunikationstjenester i offentlige net og udbyderne af informationssamfundstjenester skal føre og opretholde omfattende fortegnelser over alle sikkerhedsbrud, relevante tekniske oplysninger i den forbindelse og trufne afhjælpende foranstaltninger. Fortegnelserne skal også indeholde en henvisning til alle underretninger til abonnenter eller berørte enkeltpersoner og til de kompetente nationale myndigheder, herunder dato og indhold. Fortegnelserne skal efter anmodning forelægges den kompetente nationale myndighed.*«

— for at sikre sammenhæng i gennemførelsen af bestemmelserne om sikkerhedsbrud bør der *gives* Kommissionen mulighed for at vedtage tekniske gennemførelsesforanstaltninger efter forudgående høring af EDPS, Artikel 29-Gruppen og andre relevante interesseparter.

— med hensyn til de enkeltpersoner, der skal underrettes, bør Kommissionens eller EP's terminologi »berørte personer« eller »berørte brugere« *anvendes*, eftersom de omfatter alle enkeltpersoner, hvis personoplysninger er blevet lækket.

Offentligt tilgængelige private net

98. Ofte stilles kommunikationstjenester ikke til rådighed for offentligheden gennem offentlige net, men gennem privat drevne net (f.eks. WiFi-hotspots på hoteller og i lufthavne), der ikke er omfattet af direktivet. EP har vedtaget ændring 121 (artikel 3), der udvider direktivets anvendelsesområde til at omfatte offentlige og private kommunikationsnet såvel som offentligt tilgængelige private net. I den forbindelse bør EP og Rådet

— *bevare* substansen i ændring 121, men *omformulere* den for under e-databeskyttelsesdirektivets anvendelsesområde kun at medtage »*behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige eller offentligt tilgængelige private kommunikationsnet i Fællesskabet*«. Rent privat drevne net (i modsætning til offentligt tilgængelige private net) vil ikke blive eksplicit omfattet

— derfor *ændre* alle operationelle bestemmelser til udtrykkeligt at omhandle offentligt tilgængelige private net foruden offentlige net

— *indføje* følgende definition: »*offentligt tilgængeligt privat net: et privat drevet net, som offentligheden i almindelighed normalt har uindskrænket adgang til, uanset om det sker mod betaling eller ej eller i tilknytning til andre tjenester eller tilbud, med forbehold af accept af gældende betingelser og vilkår*«. Dette vil give større retssikkerhed med hensyn til, hvilke enheder der er omfattet af det nye anvendelsesområde

— *vedtage* en ny betragtning i henhold til hvilken Kommissionen vil gennemføre en offentlig høring om anvendelsen af e-databeskyttelsesdirektivet på alle private net, med input fra EDPS, Artikel 29-Gruppen og andre relevante interesseparter; præcisere, at Kommissionen på baggrund af den offentlige høring bør fremsætte et passende forslag om at lade flere eller færre typer enheder være omfattet af e-databeskyttelsesdirektivet.

Behandling af trafikdata af hensyn til sikkerheden

99. EP har vedtaget under førstebehandlingen ændring 181 (artikel 6, stk. 6a) om tilladelse til behandling af trafikdata af hensyn til sikkerheden. Rådet vedtog med sin fælles holdning en ny udgave, der udvandede nogle af de bestemmelser, som beskytter privatlivets fred. I den forbindelse anbefaler EDPS, at EP og Rådet

— *forkaster* denne artikel fuldstændig, fordi den er overflødig og, hvis den misbruges, kan true databeskyttelsen og privatlivets fred for enkeltpersoner

— eller, hvis en variant af den nuværende udgave af artikel 6, stk. 6a, vedtages, *indarbejder* de databeskyttelsesbestemmelser, der er omhandlet i denne udtalelse (svarende til EP's ændring).

Retssager om krænkelse af e-databeskyttelsesdirektivet

100. EP har vedtaget ændring 133 (artikel 13, stk. 6) om juridiske enheders mulighed for at indbringe spørgsmål om overtrædelse af direktivets bestemmelser for domstolene. Desværre har Rådet ikke beholdt den. Rådet og Europa-Parlamentet bør

— *godkende* den bestemmelse, der giver juridiske enheder som f.eks. forbruger- og handelsorganisationer ret til at anlægge sager om overtrædelse af direktivets bestemmelser (ikke kun overtrædelser af bestemmelserne om spam som i den nuværende udgave af den fælles holdning og det ændrede forslag). Flere forskellige håndhævelsesmekanismer vil fremme et højere overholdelsesniveau og en effektiv anvendelse af bestemmelserne i e-databeskyttelsesdirektivet som helhed.

Udfordringen

101. I samtlige ovenstående spørgsmål har EP og Rådet den udfordring, at de skal udtænke passende regler og bestemmelser, der både er brugbare og funktionelle og respekterer enkeltpersoners ret til beskyttelse af privatlivets fred og personoplysninger. EDPS har tillid til, at de involverede parter vil gøre deres yderste for at tage den udfordring op, og håber, at denne udtalelse vil bidrage hertil.

Udfærdiget i Bruxelles, den 9. januar 2009

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om forslaget til Rådets direktiv om forpligtelse for medlemsstaterne til at opretholde minimumslagre af mineralolie og/eller mineralolieprodukter

(2009/C 128/05)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser 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],

som henviser 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, særlig artikel 41 [2], og

som henviser til anmodningen om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev sendt til EDPS den 14. november 2008,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. Den 13. november 2008 vedtog Kommissionen et forslag til Rådets direktiv om forpligtelse for medlemsstaterne til at opretholde minimumslagre af mineralolie og/eller mineralolieprodukter (herefter benævnt »forslaget«) [3].

2. Forslaget har til formål at sikre et højt niveau for olieforsyningssikkerheden i Fællesskabet gennem pålidelige og gennemsigtige mekanismer baseret på solidaritet mellem medlemsstaterne og at opretholde minimumslagre af mineralolie eller mineralolieprodukter samt at indføre de nødvendige procedurer til at afhjælpe en eventuel alvorlig knaphed.

3. Den 14. november 2008 blev forslaget af Kommissionen tilsendt EDPS med henblik på en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001. EDPS hilser det velkommen, at han høres om dette spørgsmål, og noterer sig, at der henvises til denne høring i forslagets præambel, jf. artikel 28 i forordning (EF) nr. 45/2001.

4. Kommissionen havde inden vedtagelsen af forslaget uformelt hørt EDPS vedrørende en bestemt artikel i udkastet til forslag (den nuværende artikel 19). EDPS udtrykte tilfredshed med den uformelle høring, idet han derved fik lejlighed til at fremsætte bemærkninger til forslaget, inden Kommissionen vedtog det.

II. ANALYSE AF FORSLAGET

Generel analyse

5. Det foreliggende spørgsmål er et godt eksempel på, at man altid bør holde sig reglerne om databeskyttelse for øje. I en situation, der handler om medlemsstaterne og deres forpligtelse til at opbevare sikkerhedslagre af mineralolie, der hovedsagelig ejes af juridiske personer, er det ikke særlig indlysende, at der behandles personoplysninger, men selv om det ikke har været tanken, kan det alligevel godt forekomme. Man bør under alle omstændigheder overveje sandsynligheden af, at der behandles personoplysninger, og handle i overensstemmelse hermed.

6. I den foreliggende situation er der grundlæggende to aktiviteter i direktivet, der eventuelt kan indebære behandling af personoplysninger. Den første er medlemsstaternes indsamling af oplysninger om mineralolielagre og den efterfølgende videregivelse af oplysningerne til Kommissionen. Den anden aktivitet vedrører Kommissionens beføjelse til at foretage kontrol i medlemsstaterne. Indsamlingen af oplysninger om ejerne af mineralolielagre kan omfatte personoplysninger, såsom navne og kontaktoplysninger på virksomhedernes ledelse. Både indsamlingen og den efterfølgende videregivelse til Kommissionen vil da udgøre behandlingen af personoplysninger og bliver afgørende for, om det er den nationale lovgivning om gennemførelse af bestemmelserne i direktiv 95/46/EF eller forordning (EF) nr. 45/2001, der anvendes, afhængigt af hvem der faktisk behandler oplysningerne. Hvis Kommissionen får beføjelse til at kontrollere sikkerhedslagre i medlemsstaterne med beføjelse til generelt at indsamle oplysninger, kan dette også omfatte indsamling og dermed behandling af personoplysninger.

[1] EFT L 281 af 23.11.1995, s. 31.
[2] EFT L 8 af 12.1.2001, s. 1.
[3] KOM(2008) 775 endelig.

7. Under den uformelle høring, der var begrænset til bestemmelsen om Kommissionens undersøgelsesbeføjelser, rådede EDPS Kommissionen til at vurdere, om behandling af personoplysninger i forbindelse med Kommissionens undersøgelse kun vil forekomme accessorisk eller vil finde sted regelmæssigt og da som led i undersøgelsen. Alt efter resultatet af denne vurdering, blev der foreslået to fremgangsmåder.

8. Hvis behandlingen af personoplysninger ikke er planlagt og således kun forekommer accessorisk, anbefalede EDPS, at det for det første udtrykkeligt erklæres, at behandlingen af personoplysninger ikke er led i Kommissionens undersøgelse, og at det for det andet erklæres, at personoplysninger, som Kommissionen måtte støde på i forbindelse med undersøgelsen, ikke vil blive indsamlet eller inddraget, og at de, hvis de tilfældigt indsamles, omgående vil blive destrueret. Som generel supplement foreslog EDPS desuden, at der indsættes en bestemmelse om, at direktivet ikke berører reglerne om databeskyttelse i direktiv 95/46/EF og forordning (EF) nr. 45/2001.

9. Hvis det på den anden side forudses, at der regelmæssigt vil blive foretaget behandling af oplysninger i forbindelse med Kommissionens undersøgelse, anbefalede EDPS, at Kommissionen indsætter en tekst, der afspejler resultatet af en egentlig databeskyttelsesvurdering. Den bør omfatte følgende elementer: I) selve formålet med databehandlingen, II) nødvendigheden af databehandling for at opfylde dette formål og III) databehandlingens proportionalitet.

10. Skønt EDPS uformelle rådgivning kun handlede om Kommissionens undersøgelsesbeføjelser, gjaldt hans bemærkninger i lige så høj grad den anden hovedaktivitet, der redegøres for i det foreslåede direktiv, nemlig medlemsstaternes indsamling af oplysninger og videregivelse af dem til Kommissionen.

11. Det endelige direktivforslag viser klart, at Kommissionen har konkluderet, at der ikke forventes nogen behandling af personoplysninger i forbindelse med direktivet. EDPS glæder sig over, at den første af de fremgangsmåder, han har foreslået, fuldt ud kommer til udtryk i forslaget.

12. EDPS udtrykker derfor sin støtte til den måde, hvorpå Kommissionen i det foreslåede direktiv har sikret, at databeskyttelsesreglerne overholdes. Resten af denne udtalelse vil derfor kun indeholde nogle få detaljerede anbefalinger.

Bemærkninger om enkeltheder

13. Artikel 15 i det foreslåede direktiv handler om medlemsstaternes pligt til at sende Kommissionen ugentlige statistiske opgørelser over omfanget af de kommercielle lagre, der opbevares på deres nationale område. Sådanne oplysninger vil normalt kun indeholde få personoplysninger. De kan dog indeholde oplysninger om de fysiske personer, der ejer mineralolielagrene, eller som arbejder for en juridisk person, der ejer lagrene. For at forhindre, at medlemsstaterne videregiver sådanne oplysninger til Kommissionen, hedder det i artikel 15, stk. 1, at medlemsstaterne ved fremsendelsen »afholder sig fra at nævne navne på ejerne af de pågældende lagre«. Skønt man bør være klar over, at fjernelse af et navn ikke altid betyder, at oplysningerne ikke kan spores til en fysisk person, ser det ud, som om denne supplerende tekst i den foreliggende situation (statistiske opgørelser over omfanget af mineralolielagre) vil være tilstrækkelig til at sikre, at der ikke videregives personoplysninger til Kommissionen.

14. Kommissionens undersøgelsesbeføjelser findes i artikel 19 i det foreslåede direktiv. Artiklen viser klart, at Kommissionen har fulgt den første fremgangsmåde, som der er redegjort for ovenfor under punkt 8. Det fremgår, at behandling af personoplysninger ikke må indgå i Kommissionens kontrolforanstaltninger. Og selv om Kommissionen støder på sådanne oplysninger, må de ikke inddrages, og de skal destrueres i tilfælde af tilfældig indsamling. For at bringe affattelsen i overensstemmelse med affattelsen i lovgivningen om databeskyttelse og forhindre misforståelser anbefaler EDPS, at ordet »indsamling« i stk. 2, første punktum, erstattes med »behandling«.

15. EDPS udtrykker tilfredshed med, at forslaget også omfatter en generel supplerende bestemmelse om den relevante databeskyttelseslovgivning. Artikel 20 er en klar påmindelse til både medlemsstaterne, Kommissionen og andre af Fællesskabets organer om deres forpligtelser ifølge henholdsvis direktiv 95/46/EF og forordning (EF) nr. 45/2001. Bestemmelsen understreger desuden de rettigheder, de registrerede har i henhold til disse bestemmelser, såsom retten til at gøre indsigelse mod behandling af oplysninger om dem, retten til indsigt i oplysninger om dem og retten til berigtigelse af fejlagtige oplysninger om dem. Det er måske på sin plads at gøre en enkelt bemærkning til denne bestemmelses placering i forslaget. Det er en generel bestemmelse, og den gælder således ikke kun for Kommissionens undersøgelsesbeføjelser. EDPS anbefaler derfor at flytte artiklen til direktivets begyndelse, f.eks. efter artikel 2.

16. Der henvises også i betragtning 25 til direktiv 95/46/EF og forordning (EF) nr. 45/2001. Formålet med betragtningen er imidlertid temmelig uklart, da der kun nævnes databeskyttelseslovgivningen som sådan uden nogen nærmere redegørelse. Det bør fremgå klart af betragtningen, at direktivets bestemmelser ikke berører den nævnte lovgivning. Desuden antyder betragtningens sidste punktum, at databeskyttelseslovgivningen udtrykkeligt kræver, at den registeransvarlige omgående destruerer personoplysninger, der indsamles tilfældigt. Skønt det kan blive en konsekvens af de fastsatte regler, findes der ikke en sådan forpligtelse

i den pågældende lovgivning. Det er et generelt databeskyttelsesprincip, at personoplysninger ikke opbevares længere, end det er nødvendigt for de formål, hvortil de er indsamlet eller behandles yderligere. Hvis den første del af betragtningen justeres, således som det foreslås, bliver sidste punktum overflødigt. EDPS foreslår derfor at lade sidste punktum i betragtning 25 udgå.

III. **KONKLUSION**

17. EDPS ønsker at udtrykke sin støtte til den måde, hvorpå Kommissionen i det foreslåede direktiv har sikret, at databeskyttelsesreglerne overholdes.

18. På et mere detaljeret plan anbefaler EDPS følgende:

— at erstatte ordet »indsamling« i artikel 19, stk. 2, første punktum, med ordet »behandling«

— at flytte artikel 20, der er den generelle bestemmelse om databeskyttelse, til direktivets begyndelse, nemlig lige efter artikel 2

— at indsætte en passage i betragtning 25, om at direktivets bestemmelser ikke berører bestemmelserne i direktiv 95/46/EF og forordning (EF) nr. 45/2001

— at lade sidste punktum i betragtning 25 udgå.

Udfærdiget i Bruxelles, den 3. februar 2009

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

IV

(Oplysninger)

OPLYSNINGER FRA DEN EUROPÆISKE UNIONS INSTITUTIONER OG ORGANER

KOMMISSIONEN

Euroens vekselkurs [1]

5. juni 2009

(2009/C 128/06)

1 euro =

	Valuta	Kurs		Valuta	Kurs
USD	amerikanske dollar	1,4177	AUD	australske dollar	1,7606
JPY	japanske yen	137,48	CAD	canadiske dollar	1,5657
DKK	danske kroner	7,4472	HKD	hongkongske dollar	10,9887
GBP	pund sterling	0,87920	NZD	newzealandske dollar	2,2263
SEK	svenske kroner	10,9250	SGD	singaporeanske dollar	2,0530
CHF	schweiziske franc	1,5191	KRW	sydkoreanske won	1 768,65
ISK	islandske kroner		ZAR	sydafrikanske rand	11,4189
NOK	norske kroner	8,9700	CNY	kinesiske renminbi yuan	9,6871
BGN	bulgarske lev	1,9558	HRK	kroatiske kuna	7,3550
CZK	tjekkiske koruna	27,003	IDR	indonesiske rupiah	14 078,75
EEK	estiske kroon	15,6466	MYR	malaysiske ringgit	4,9556
HUF	ungarske forint	289,10	PHP	filippinske pesos	67,016
LTL	litauiske litas	3,4528	RUB	russiske rubler	43,5789
LVL	lettiske lats	0,7094	THB	thailandske bath	48,464
PLN	polske zloty	4,5420	BRL	brasilianske real	2,7345
RON	rumænske leu	4,2185	MXN	mexicanske pesos	18,7066
TRY	tyrkiske lira	2,1834	INR	indiske rupee	66,7910

[1] *Kilde*: Referencekurs offentliggjort af Den Europæiske Centralbank.

BERIGTIGELSER

Berigtigelse til Den Europæiske Centralbanks rentesats for de vigtigste refinansieringstransaktioner

(Den Europæiske Unions Tidende C 124 af 4. juni 2009)

(2009/C 128/07)

I indholdsfortegnelsen på omslaget og side 1, titlen:

I stedet for: »1,00 % pr. 4. juni 2009«

læses: »1,00 % pr. 1. juni 2009.«

ABONNEMENTSPRISER 2009 (ekskl. moms, inkl. normale forsendelsesomkostninger)

EU-Tidende, L- + C-udgaven, kun papirudgave	22 officielle EU-sprog	1 000 EUR pr. år (*)
EU-Tidende, L- + C-udgaven, kun papirudgave	22 officielle EU-sprog	100 EUR pr. måned (*)
EU-Tidende, L- + C-udgaven, papirudgave + årlig cd-rom	22 officielle EU-sprog	1 200 EUR pr. år
EU-Tidende, L-udgaven, kun papirudgave	22 officielle EU-sprog	700 EUR pr. år
EU-Tidende, L-udgaven, kun papirudgave	22 officielle EU-sprog	70 EUR pr. måned
EU-Tidende, C-udgaven, kun papirudgave	22 officielle EU-sprog	400 EUR pr. år
EU-Tidende, C-udgaven, kun papirudgave	22 officielle EU-sprog	40 EUR pr. måned
EU-Tidende, L- + C-udgaven, månedlig kumulativ cd-rom	22 officielle EU-sprog	500 EUR pr. år
Supplement til EUT (S-udgaven), udbud og offentlige kontrakter, cd-rom, 2 udgaver pr. uge	Flersproget: 23 officielle EU-sprog	360 EUR pr. år (= 30 EUR pr. måned)
EU-Tidende, C-udgaven — udvælgelsesprøver	Sprog iht. udvælgelsesprøve(r)	50 EUR pr. år

(*) Enkeltnumre: til og med 32 sider: 6 EUR
fra 33 til og med 64 sider: 12 EUR
over 64 sider: Prisen fastsættes i hvert enkelt tilfælde.

Den Europæiske Unions Tidende, der udkommer på EU's officielle sprog, fås i abonnement i 22 sprogudgaver. EU-Tidende omfatter L-udgaven (retsforskrifter) og C-udgaven (meddelelser og oplysninger).

Der abonneres særskilt på hver sprogudgave.

I henhold til Rådets forordning (EF) nr. 920/2005, offentliggjort i EU-Tidende L 156 af 18. juni 2005, er Den Europæiske Unions institutioner midlertidigt fritaget for forpligtelsen til at udarbejde og offentliggøre alle retsakter på irsk. Irske udgaver af EU-Tidende vil derfor blive markedsført særskilt.

Abonnementet på supplementet til EU-Tidende (S-udgaven (udbud og offentlige kontrakter)) omfatter alle udgaver på de 23 officielle sprog på én cd-rom.

Abonnenter på *Den Europæiske Unions Tidende* kan uden ekstra omkostninger rekvirere eksemplarer af diverse bilag til EU-Tidende (C … A-udgaver). Abonnenterne gøres opmærksom på udgivelsen af bilagene ved hjælp af »meddelelser til læserne« i *Den Europæiske Unions Tidende*.

Salg og abonnementer

Publikationer, der er produceret af Kontoret for De Europæiske Fællesskabers Officielle Publikationer (Publikationskontoret) med salg for øje, kan købes gennem vore salgsagenter. Listen over salgsagenterne findes på internettet:

http://publications.europa.eu/others/agents/index_da.htm

EUR-Lex (http://eur-lex.europa.eu) giver direkte og gratis adgang til EU-retten. Via dette netsted kan man konsultere *Den Europæiske Unions Tidende*, og netstedet indeholder endvidere traktaterne, retsforskrifter, retspraksis og forberedende retsakter.

Yderligere oplysninger om Den Europæiske Union findes på: http://europa.eu

Publikationskontoret
Publications.europa.eu

KONTORET FOR DE EUROPÆISKE FÆLLESSKABERS OFFICIELLE PUBLIKATIONER
L-2985 LUXEMBOURG

DA