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